IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

PATRICIA POWERS, on behalf of herself and all others similarly situated, ***Plaintiff,*** **v.** **BLUE CROSS AND BLUE SHIELD OF ILLINOIS INC.** ***Defendant.***	**Case No.:** **JURY TRIAL DEMANDED**

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff PATRICIA POWERS (hereinafter, "Plaintiff"), brings this action, on behalf of herself and all others similarly situated, for causes of action against Defendant BLUE CROSS AND BLUE SHIELD OF ILLINOIS INC. ("Defendant" or "BCBSIL"), and alleges upon personal knowledge as to her own actions, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This action arises out of Defendant's unauthorized disclosure of the confidential Personally Identifying Information[1] ("PII" or "Private Information") of Plaintiff and the proposed Class Members (the "Data Breach"), including their names, dates of birth, group numbers, subscriber numbers, addresses, phone numbers, claim numbers (DCN), medical services information, and Social Security Numbers.

[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. BCBSIL is Illinois' only statewide, customer-owned health insurer. BCBSIL is the largest provider of health benefits in Illinois, serving more than 8.9 million members in all 102 counties across the state. For more than 85 years, BCBSIL has provided its members with comprehensive, affordable health plans.

3. On June 15, 2023, BCBSIL discovered that Plaintiff and Class Members' PII was disclosed to an unauthorized third party during the period September 19, 2022 through May 18, 2023. Plaintiff and Class Members' PII was disclosed through an unnamed third party vendor of BCBSIL. It took BCBSIL nearly 9 months to discover the Data Breach, and nearly a full year to inform impacted individuals that their PII was disclosed to an unauthorized third party.

4. On information and belief, BCBSIL failed to undertake adequate measures to safeguard the PII of Plaintiff and the proposed Class Members, including by failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

5. As a direct and proximate result of Defendant's failures to protect Plaintiff's and the Class Members' sensitive PII and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

PARTIES

6. Plaintiff Patricia Powers is a resident and citizen of California. Plaintiff received a letter, dated September 5, 2023, from Blue Cross Blue Shield of Illinois notifying Plaintiff that her PII was involved in the Data Breach.

7. BCBSI is a corporation organized under the laws of California with its headquarters located at 300 East Randolph Street, Chicago, Illinois 60601.

JURISDICTION AND VENUE

8. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in this state; it maintains its principal places of business and headquarters in Illinois; and committed tortious acts in Illinois.

9. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

10. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law under 28 U.S.C. § 1367.

11. Venue is proper under 28 U.S.C. § 1391(b)(1) and (2) because Defendant resides in this district and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this district.

FACTUAL BACKGROUND

A. Defendant BCBSIL

12. BCBSIL is the largest provider of health benefits in Illinois.

13. Defendant collected PII from its customers who contract with them for health insurance policies and coverage.

14. On or around mid-June 2023, Defendant became aware of a cybersecurity incident. However, Defendant has provided very few details publicly and/or any specific information about the incident to Plaintiff and/or Class Members. Defendant issued a vague

Notice of Data Breach on September 5, 2023 to impacted individuals, including to Plaintiff.

15. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the proposed Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff, and the members of the Proposed Class, and knew or should have known that they were responsible for protecting their PII from unauthorized disclosure.

16. At all times, Plaintiff has taken reasonable steps to maintain the confidentiality of their PII, and Plaintiff relied on Defendant to keep their PII confidential and securely maintained.

B. BCBSIL Fails to Adequately Safeguard PII

17. Defendant did not have adequate security protocols to prevent, detect, and stop the Data Breach and allowing the PII of Plaintiff and the proposed Class Members to be accessed by unauthorized individuals.

18. Further, BCBSIL failed to adequately train their employees on reasonable cybersecurity protocols and failed to implement reasonable security measures, causing it to lose control over individuals' PII in the Data Breach.

19. Defendant's tortious conduct and breach of contractual obligations, as explained hereinafter, are evidenced by their failure to recognize the Data Breach for nearly 9 months, meaning BCBSIL had no effective means to detect and prevent attempted data breaches.

20. As a result of BCBSIL's Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their Social Security numbers. Accordingly, BCBSIL's identity theft protection offered to impacted individuals is wholly insufficient to compensate Plaintiff and the Class Members for their damages caused by the Data Breach.

21. Indeed, as a result of the Data Breach which Defendant permitted to occur by virtue of their inadequate data security practices, Plaintiff and the proposed Class Members have suffered injury and damages, as set forth herein.

C. Plaintiff's Experience

22. Plaintiff's sensitive PII was entrusted and disclosed to BCBSIL directly or indirectly, in connection with Defendant's provision of health insurance to Plaintiff.

23. Plaintiff received a Data Beach Notice from Blue Cross Blue Shield dated September 5, 2023, informing her that her name, date of birth, group number, subscriber number, address, phone number, claim number (DCN), medical services information, and Social Security Number had been compromised in the Data Breach.

24. To her knowledge, Plaintiff has never been the victim of a prior data breach.

25. As a direct result of the Data Breach, Plaintiff has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of her PII that can be directly traced to Defendant.

26. On information and belief, Plaintiff's PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

27. Plaintiff has spent time mitigating the effects of the Data Breach by researching the Data Breach and checking her accounts for unauthorized activity.

28. In addition, Plaintiff must now spend time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring her credit reports, and fears for her personal financial security and uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the

Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

29. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PII and the harm caused by the Data Breach.

30. As a result of BCBSIL's Data Breach, Plaintiff faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like her Social Security number.

D. This Data Breach was Foreseeable by BCBSIL.

31. Plaintiff's and the proposed Class Members' PII was provided to BCBSIL with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

32. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the PII of Plaintiff and the Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

33. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

34. Cyber-attacks against companies such as Defendant are targeted and frequent. Indeed, according to UpGuard, "[c]ybercriminals know that tech companies often have weaker

data protection and overall cybersecurity measures than highly-regulated industries, like healthcare and finance. Instead of targeting these organizations directly for their valuable data, they focus their efforts on the poor data security often found in the first link of the supply chain – tech vendors that store and manage significant amounts of data from these industries."[2]

35. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[3]

36. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including BCBSIL. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[4]

37. Based on data from the Maine Attorney General, as of August 2022, "…at least 79 financial service companies have reported data breaches affecting 1,000 or more consumers, and the total number of consumers affected by these breaches could be as high as 9.4 million."[5]

---

[2] UpGuard, Catherine Chipeta, "5 Ways Tech Companies Can Prevent Data Breaches," updated Mar. 2, 2023 available at https://www.upguard.com/blog/how-tech-companies-can-prevent-data-breaches (last acc. Jun. 15, 2023).

[3] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Apr. 14, 2023).

[4] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Apr. 14, 2023).

[5] Carter Pape, "Breach data from Maine shows scope of bank, credit union exposures," American Banker, August 24, 2022, available at https://www.americanbanker.com/news/breach-data-from-maine-shows-scope-of-bank-credit-union-exposures

38. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

39. PII can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

40. Given the nature of the Data Breach, it was foreseeable that the compromised PII could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and the Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in the Class Members' names.

E. BCBSIL Failed to Comply with FTC Guidelines

41. The Federal Trade Commission ("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 business decision-making.

42. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it

occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[6]

43. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[7]

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

45. These FTC enforcement actions include actions against insurance companies for failing to safeguard PII, like Defendant.

46. BCBSIL failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

47. Defendant was at all times fully aware of its obligation to protect the PII of

[6] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).
[7] *See id*.

Plaintiff and the Class Members. BCBSIL was also aware of the significant repercussions that would result from their failure to do so.

F. BCBSIL Fails to Comply with Industry Standards

48. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

49. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[8]

50. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.

[8] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. June 8, 2023).

- Have formal policies for safely disposing of electronic files and old devices.

- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[9]

51. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (1) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (2) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (3) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[10]

52. Upon information and belief, BCBSIL failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST

[9] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).

[10] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. June 8, 2023).

Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiff's and the proposed Class Members' PII, resulting in the Data Breach.

G. The Data Breach Caused Plaintiff and Class Members to Suffer Injuries and Damages

53. Plaintiff and members of the proposed Class have suffered injury and damages from the misuse of their PII that can be directly traced to BCBSIL, and that has occurred, is ongoing, and/or imminently will occur.

54. As stated prior, in the Data Breach, an unauthorized third party was able to access the Plaintiff's and the proposed Class Members' PII, which is now available to be imminently used for fraudulent purposes or has been sold for such purposes, causing widespread injury and damages.

55. The ramifications of BCBSIL's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

56. Because BCBSIL failed to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class Members have suffered, will imminently suffer, or are at an increased risk of suffering:

a. Fraudulent misuse of PII;

b. The loss of the opportunity to control how PII is used;

c. The diminution in value of their PII;

d. The compromise and continuing publication of their PII;

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

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

g. Delay in receipt of tax refund monies;

h. Increase in spam texts and telephone calls;

i. Unauthorized use of stolen PII; and

j. The continued risk to their PII, which remains in the possession of BCBSIL and is subject to further breaches so long as BCBSIL fails to undertake the appropriate measures to protect the PII in their possession.

57. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

58. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud;

theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[11]

59. The FTC recommends that identity theft victims take time and effort intensive or costly steps to protect their personal and financial information after a data breach, including contacting the company where the fraud occurred and asking them to close or freeze accounts and changing login information; contacting one of the credit bureaus to place a fraud alert on credit files (consider an extended fraud alert that lasts for 7 years if someone steals their identity); reviewing their credit reports; seeking a credit freeze; correcting their credit reports; and other steps such as contacting law enforcement and reporting the identity theft to the FTC.[12]

60. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud—just as occurred here—phone or utilities fraud, and bank/finance fraud.

61. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

---

[11] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Feb. 27, 2023).

[12] *See* Federal Trade Commission, available at https://www.identitytheft.gov/Steps (last acc. June 8, 2023).

62. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive other services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

63. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. 35% reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. 54% percent reported feelings of being violated. [13]

64. What's more, theft of PII is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, PII is valuable property.[14]

65. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PII has considerable market value.

---

[13] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Feb. 27, 2023).

[14] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, 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).

66. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

67. PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

68. Where the most PII belonging to Plaintiff and Class Members was accessible from BCBSIL's network, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and the Class Members must vigilantly monitor their financial accounts for many years to come.

69. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[15]

70. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for

[15] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023)

unemployment benefits, or apply for a job using a false identity.[16] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

71. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

72. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

73. BCBSIL knew or should have known of these harms which would be caused by the Data Breach they permitted to occur, and strengthened their data systems accordingly.

CLASS ALLEGATIONS

114. Plaintiff incorporates by reference all other paragraphs of this Complaint as if

---

[16] *See id.*

[17] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

[18] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 13, 2023).

fully set forth herein.

115. Plaintiff brings this nationwide class action on behalf of herself individually and on behalf of all other persons similarly situated pursuant to Rule 23(a) of the Federal Rules of Civil Procedure, and Fed. R. Civ. P. 23(b)(3).

116. Plaintiff proposes the following Class definition (the "Class"), subject to amendment based on information obtained through discovery:

> **Nationwide Class**
> **All persons whose PII was compromised as a result of the Data Breach experienced by BCBSIL beginning on or about September 19, 2022, including all persons who received Defendant's Data Breach Notice.**

117. In addition, or in the alternative, Plaintiff proposes the following State Class definition, subject to amendment as appropriate:

> **California Subclass:**
> **All California residents whose PII was compromised as a result of the Data Breach experienced by BCBSIL beginning on or about September 19, 2022, including all persons who received Defendant's Data Breach Notice (the "California Subclass").**

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

119. Plaintiff reserves the right to amend the definition of the Class and/or California Subclass or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

120. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members' claims on a class-wide basis using the same

evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

121. This action satisfies the requirements for a class action under Fed. R. Civ. P. 23(a)(1)-(3) and Fed. R. Civ. P. 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

122. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, it is likely that the PII of several thousands of individuals was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

123. **Commonality, Fed. R. Civ. Proc. 23(a)(2), and Predominance, Fed. R. Civ. Proc. 23(b)(3):** There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the Members of the Class. These questions predominate over questions that may affect only individual Class Members because BCBSIL has acted on grounds generally applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

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

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

d. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

e. Whether computer hackers obtained Plaintiff's and Class Members' PII in the Data Breach;

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

g. Whether BCBSIL failed to adequately respond to the Data Breach, including failing to timely notify the Plaintiff and the Class Members;

h. Whether Defendant's failures amounted to negligence;

i. Whether Defendant breached their contractual promises;

j. Whether Defendant were unjustly enriched;

k. Whether Defendant intruded into the private affairs of Plaintiff and the Class Members;

l. Whether Plaintiff and the Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

m. Whether Defendant's acts violated the law, and;

n. Whether Plaintiff and the Class Members are entitled to damages including compensatory and punitive damages, and/or injunctive relief.

124. **Typicality, Fed. R. Civ. P. 23(a)(3):** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was

compromised in the Data Breach, and all arise from the same set of facts regarding BCBSIL's failures:

a. to protect Plaintiff's and Class Members' PII;

b. to discover and remediate the security breach of its computer systems more quickly; and

c. to disclose to Plaintiff and Class Members in a complete and timely manner information concerning the security breach and the theft of their Personal Information.

125. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

126. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be

able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendants.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only BCBSIL's client's customers, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be

appropriate.

127. **Injunctive and Declaratory Relief, Fed. R. Civ. Proc. 23(b)(2):** In addition, Defendant have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

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

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

129. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

130. Defendant collected the PII of Plaintiff and the proposed Class Members and stored this information in their computer information technology systems.

131. Defendant had full knowledge of the sensitivity of the PII to which they were entrusted, and the types of harm that Plaintiff and the Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information.

132. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their data in Defendant's possession.

133. By collecting and storing this data in their computer systems, Defendant had a

duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that PII was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

134. Defendant owed a common law duty of care to Plaintiff and the Class Members to provide adequate 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 PII.

135. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

136. Defendant breached its duties, and was negligent, by acts of omission or commission, by failing to use reasonable measures to protect the Plaintiff's and Class Members' PII. 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 Plaintiff's and Class Members' PII;

b. Failing to adequately train employees on proper cybersecurity protocols;

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

d. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff's and Class Members' PII;

f. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

137. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

138. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in one or more types of injuries to them.

139. As a direct and proximate result of Defendant's negligence set forth in the preceding paragraphs, Plaintiff and Class Members have suffered injury and damages as set forth herein, including but not limited to fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to compensatory, actual, and punitive damages as a result of the Data Breach.

140. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their 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
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

141. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

142. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for Defendant to provide administrative services in connection with their health insurance policies and programs, and that Defendant would deal with them fairly and in good faith, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII entrusted to Defendants.

143. Specifically, Plaintiff and the Class Members entered into valid and enforceable implied contracts with Defendant when they first received Defendant's services.

144. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promise to protect nonpublic PII given to Defendant, or that Defendant created on their own, from unauthorized disclosures. Plaintiff and Class Members allowed their PII to be provided in reliance of that promise.

145. Defendant solicited and invited Plaintiff and Class Members to provide their PII, directly or indirectly, as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendants.

146. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

147. Plaintiff and Class Members reasonably believed and expected that Defendant would adequately employ adequate data security to protect that PII. Defendant failed to do so.

148. Under the implied contracts, Defendant promised and were obligated to: (a) provide services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII: (i) provided to obtain such services and/or (ii) created in connection therewith.

In exchange, Plaintiff and Class Members agreed to pay money for these services and to turn over their PII.

149. Both the provision of these services, and the protection of Plaintiff's and Class Members' PII, were material aspects of these implied contracts.

150. Plaintiff and Class Members would not have entrusted their PII to Defendant and entered into these implied contracts with Defendant without an understanding that their PII would be safeguarded and protected, or entrusted their PII to Defendant, directly or indirectly, in the absence of their implied promise to monitor their computer systems and networks to ensure that PII was not disclosed to unauthorized parties and exposed to the public as occurred in the Data Breach.

151. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their PII to Defendant and paid for services for, amongst other things, (a) the provision of such services and (b) the protection of their PII.

152. Plaintiff and the Class Members performed their obligations under the contracts when they paid for services, directly or indirectly, and provided their PII to Defendants.

153. Defendant materially breached their contractual obligations to protect the nonpublic PII of Plaintiff and the Class Members which Defendant required and gathered when the information was unauthorized disclosed in the Data Breach.

154. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these contracts.

155. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains, and instead received services that were of a diminished value compared to those described in

the contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

156. Had Defendant disclosed that their security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased services from Defendant.

157. As a direct and proximate result of the Data Breach, Plaintiff and the Class Members have suffered injury and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they had struck with Defendant.

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

159. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Breach Of Contract—Third Party Beneficiary
(On Behalf of Plaintiff and the Class)

160. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

161. Plaintiff brings this claim in the alternate to her claim for Breach of Implied Contract (Count II).

162. Defendant entered into valid and enforceable contracts with third party vendors to

assist in administering their plans and/or portions of their plans, in exchange for payment, and which included obligations for third party vendors and Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII entrusted to Defendant.

163. Defendant solicited and paid money to third party vendors for their assistance in administering their plans, which involved the access to Plaintiff's and Class Members' PII, as part of Defendant's regular business practices.

164. Both the provision of these services and payment, and the protection of Plaintiff's and Class Members' PII, were material aspects of these contracts.

165. Plaintiff and the Class Members were the intended beneficiaries of these contracts as facilitating their participation in administration of their health care plans.

166. These valid and enforceable contracts included Defendant's promise to protect nonpublic PII of Plaintiff and Class Members given to Defendant, or that Defendant created on their own, from unauthorized disclosures. Plaintiff and Class Members allowed their PII to be provided in reliance of that promise.

167. Defendant materially breached their contractual obligations to protect the nonpublic PII of Plaintiff and the Class Members which Defendant required and gathered when the information was unauthorized disclosed in the Data Breach.

168. Defendant materially breached their contractual obligations to deal fairly and in good faith with Plaintiff and the Class Members when they failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

169. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these contracts of which Plaintiff and

the Class Members were the intended beneficiaries.

170. As a result of Defendant's failure to fulfill the data security protections promised in these contracts in which Plaintiff and the Class Members were the intended beneficiaries, Plaintiff and Class Members have suffered injury and damages as set forth herein and have been irreparably harmed.

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

172. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

173. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

174. Plaintiff and proposed Class Members conferred benefits upon Defendant in the form of monies received by BCBSIL, and in the form of valuable PII entrusted to Defendants.

175. Defendant appreciated or knew of these benefits that they received. And under principles of equity and good conscience, this court should not allow Defendant to retain the full value of these benefits—specifically, the monies, and PII of Plaintiff and members of the Class.

176. Defendant failed to adequately protect Plaintiff's and Class Members' PII. And if such inadequacies were known, then Plaintiff and the members of the Class would never have

conferred payment to Defendant, nor disclosed their PII.

177. As a result of Defendant's wrongful conduct as alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class Members.

178. As a direct and proximate result of Defendant's unjust enrichment set forth in the preceding paragraphs, Plaintiff and Class Members have suffered injury and damages as set forth herein, including but not limited to fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to damages as a result of the Data Breach.

179. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein.

180. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to retain the benefits they received, and are still receiving, without justification, from Plaintiff and Class Members in an unfair, unconscionable, and oppressive manner. Defendant's retention of such funds under circumstances making it inequitable to do so constitutes unjust enrichment.

181. The financial benefits derived by Defendant rightfully belong to Plaintiff and Class Members. Defendant should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all wrongful or inequitable proceeds collected by Defendant. A constructive trust should be imposed upon all wrongful or inequitable sums received by Defendant traceable to Plaintiff and Class Members.

182. Plaintiff and the Class Members have no adequate remedy at law.

COUNT V
Violations of the California Consumer Privacy Act Of 2018
Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiff and the California Subclass)

183. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein and brings this count on behalf of herself and the California Subclass (the "Class" for the purposes of this count).

184. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

185. As a result, in 2018, the California Legislature passed the California Consumer Privacy Act of 2018 ("CCPA"), giving consumers broad protections and rights intended to safeguard their personal information.

186. Among other things, the CCPA, Cal. Civ. Code §§ 1798.100(e), imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

187. On information and belief, BCBSIL is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

188. Section 1798.150(a)(1) of the CCPA provides: "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for"

statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

189. Through the above-detailed conduct, Defendant violated the CCPA by subjecting the nonencrypted and nonredacted PII of Plaintiff and Class Members to unauthorized access and exfiltration, theft, or disclosure as a result of BCBSIL's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

190. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g) because he is natural person residing in the state of California.

191. On information and belief, Defendant are each a "business" as defined by Civ. Code § 1798.140(c) because each are a legal entity that does business in the state of California and have annual revenues of in excess of $25,000,000.

192. The CCPA provides that "personal information" includes "[i]dentifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers." *See* Civ. Code § 1798.140.

193. Plaintiff's PII compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

194. Through the Data Breach, Plaintiff's PII was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

195. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

196. Concurrent with the filing of this Complaint, will provide a separate notice letter to Defendant pursuant to Cal. Civ. Code § 1798.150(b) identifying the specific provisions of the CCPA Plaintiff alleges Defendant has violated or is violating. Although a cure is not possible under the circumstances, if (as expected) Defendant are unable to cure or does not cure the violation within 30 days, Plaintiff will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

COUNT VI
Violation Of California's Consumer Records
Cal. Civ. Code §§ 1798.82, *et seq.* ("CCRA")
(On Behalf of Plaintiff and the California Class)

197. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein and brings this count on behalf of herself and the California Subclass (the "Class" for the purposes of this count).

198. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under Section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay…"

199. The CCRA further provides: "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data *immediately* following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b) (emphasis

added).

200. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

> (A) The name and contact information of the reporting person or business subject to this section.
>
> (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
>
> (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
>
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
>
> (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
>
> (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
>
> (G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

Cal. Civ. Code § 1798.82(d)(2).

201. The Data Breach described herein constitutes a "breach of the security system" of

BCBSIL.

202. As alleged herein, it took nearly a full year for Defendant to begin informing Plaintiff and the Class or California Class Members about the Data Breach. BCBSIL unreasonably delayed information to Plaintiff and Class Members about the Data Breach, affecting their PII, after Defendant knew the Data Breach had occurred.

203. Defendant failed to disclose to Plaintiff and California Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII, when BCBSIL knew or reasonably believed such information had been compromised.

204. Defendant's ongoing business interests gave BCBSIL incentive to conceal the Data Breach from the public to ensure continued revenue.

205. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and California Class Members would impede its investigation.

206. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and the California Class Members or Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class Members because their PII would have had less value to identity thieves.

207. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and the California Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

208. Plaintiff and California Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to, to the damages suffered by Plaintiff and Class Members as alleged above and equitable relief.

209. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to BCBSIL conducted with the intent on the part of Defendant depriving Plaintiff and Class Members of "legal rights or otherwise causing injury."

210. In addition, Defendant's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c) in that it was despicable conduct carried on by BCBSIL with a willful and conscious disregard of the rights or safety of Plaintiff and Class Members and despicable conduct that has subjected Plaintiff and Class Members to cruel and unjust hardship in conscious disregard of their rights.

211. As a result, Plaintiff and Class Members are entitled to punitive damages under Cal. Civ. Code § 3294(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself, and all others similarly situated, prays for judgment as follows:

A. Trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable;

B. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class and California Subclass, appointing Plaintiff as class representative, and appointing their counsel to represent the Class and California Subclass;

C. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and statutory damages, and punitive damages, as allowed

by law;

D. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

E. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

G. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the transmitted PII;

H. Awarding attorneys' fees and costs, as allowed by law;

I. Awarding prejudgment and post-judgment interest, as provided by law;

J. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

K. Any and all such relief to which Plaintiff and the Class are entitled.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: October 3, 2023

Respectfully submitted,

/s/ Gary M. Klinger
Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

Jason M. Wucetich*
WUCETICH & KOROVILAS, LLP
222 N. PCH Blvd., Suite 2000
El Segundo, CA 90245
(310) 335-2001
(310) 364-5201 (facsimile)
jason@wukolaw.com

**Pro Hac Vice* application forthcoming

Counsel for Plaintiff and
the Proposed Class

ClassAction.org