IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

JOHN BERRY, individually and on behalf of all others similarly situated, Plaintiffs, v. REFRESCO BEVERAGES U.S. INC., Defendant.	**Case No.: 8:23-cv-02763-TPB-SPF** **JURY TRIAL DEMANDED**

AMENDED CLASS ACTION COMPLAINT

Plaintiff John Berry ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant Refresco Beverages U.S. Inc. ("Refresco" or "Defendant"), upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This is a class action for damages with respect to Refresco, for its failure to exercise reasonable care in securing and safeguarding its employees' sensitive personal data—including: name, date of birth, Social Security numbers, street address, financial account number, driver's license number (personally

identifying information" or "PII") and health insurance policy number, and certain health information as provided in connection with workers' compensation and/or ADA accommodations proceedings, which is protected health information ("PHI", and collectively with personally identifiable information, "Private Information" as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPPA").

2. Upon information and belief, former and current Refresco employees are required to entrust Defendant with sensitive, non-public Private Information, without which Defendant could not perform its regular business activities, in order to obtain medical coverage from Refresco. Defendant retains this information for years and even after the employer-employee relationship has ended.

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

4. Defendant's data security failure allowed a targeted cyberattack in or about March 2023 to compromise Defendant's network (the "Data Breach") that contained Private Information of Plaintiff and other individuals.

5. The Defendant sent notice to the Attorney General of Maine on or about

May 14, 2023, that the individuals affected numbered 25,170.[1]

6. According to its notice, Defendant confirmed that the "cybersecurity incident" occurred, but has no exact date as to when beyond March 2023.

7. Defendant's notice states, in part: "Late in the day on May 14, 2023, Refresco learned that it had experienced a cyber incident involving unauthorized third-party access to portions of our North American network systems. We immediately brought in a top cybersecurity investigation firm and experienced legal counsel to conduct a comprehensive investigation."[2]

8. Despite learning of the Data Breach on or about May 14, 2023, and determining that Private Information was involved in the March 2023, Defendant claims it did not begin sending notices of the Data Breach (the "Notice Letter") until November 9, 2023.

9. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect its employees' data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims

[1] Consumer Notice Refresco-Letter-US_Redacted (1).pdf (last accessed Nov. 29, 2023)
[2] *Id.*

of the Data Breach will remain for their respective lifetimes.

10. The Data Breach was a direct consequence of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for either employment or health coverage or both.

11. Since the data breach started—on or about March 2023—Plaintiff and Class Members were unaware that their sensitive Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

12. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents.

13. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and

appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class members was compromised through disclosure to an unknown and unauthorized third party.

14. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

15. Plaintiff and Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time, spent on activities remedying harms resulting from the Data Breach; (iv) an increase in spam calls, texts, and/or emails; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) diminution of value of their Private Information; and (vii) the continued and increased risk of fraud and identity theft.

16. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

17. John Berry was, at all relevant times, a resident and citizen of Redlands, California. Mr. Berry is a former employee of Defendant's who was employed by

Cott Beverage when it was acquired by Defendant, between Dec. 2015 to Feb. 2018.

18. Mr. Berry provided his Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Mr. Berry had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

19. Defendant Refresco Beverages U.S. Inc. is a beverages company incorporated under the state laws of Georgia, with its principal place of business located in 8112 Woodland Center Blvd., Tampa, FL 33614.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action 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 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

21. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

22. Venue is proper under 18 U.S.C. § 1391 because Defendant's principal

place of business is in this District.

FACTUAL ALLEGATIONS

Defendant's Business

23. Defendant is a beverages company that manufactures, packages, and distributes various beverages throughout the United States, offering carbonated soft drinks, juices, smoothies, sparkling and flavored waters, sport drinks, ready-to-drink tea, and other non-carbonated beverages."

24. Defendant has "more than 70 production locations across Europe, North America and Australia."[3]

25. Plaintiff and Class Members are current and former Refresco employees.

26. In order to obtain employment and medical coverage through Refresco, Plaintiff and Class Members were required to provide sensitive and confidential Private Information, including: name, date of birth, Social Security numbers, street address, financial account number, driver's license number, health insurance policy number, and certain health information as provided in connection with workers' compensation and/or ADA accommodations proceedings.

27. The information held by Defendant in its computer systems included the unencrypted Private Information of Plaintiff and Class Members.

---

[3] [3] https://www.refresco.com/en/about-us/where-we-operate (last accessed Nov. 29, 2023)

28. Upon information and belief, Defendant's HIPAA Notice of Privacy Practices ("Privacy Policy") is provided to every employee both prior to receiving coverage and upon request.

29. Defendant's Privacy Notice makes clear that it understands that its employees' and applicants' Private Information is personal and must be protected by law.

30. Indeed, Defendant's Privacy Policy provides that: "It is Refresco's policy to comply with the privacy legislation within each jurisdiction in which we operate."[4]

31. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff and Class Members in a safe and confidential manner, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

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

33. Yet, through its failure to properly secure the Private Information of

[4] https://www.refresco.com/en/privacy (last accessed Sept. 14, 2023).

Plaintiff and Class Members, Defendant failed to meet its own promises of employee privacy.

34. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

The Data Breach

36. According to Defendant's notice, it learned of a cyberattack on its computer systems on or around March 2023, when it took many of its "North American network systems" offline, adversely affecting employee treatment, scheduling, and the ability to access employee histories.[5]

37. Defendant notified the Attorney General of Maine of the Data Breach on or about May 14, 2023, listing 25,170 affected individuals.

38. On or about November 9, 2023, months after Defendant learned of the Data Breach, Defendant began sending the Notice Letter to Class Members, informing them that:

[5] Consumer Notice Refresco-Letter-US_Redacted (1).pdf (last accessed Nov. 29, 2023).

> **What Happened?** Late in the day on May 14, 2023, Refresco learned that it had experienced a cyber incident involving unauthorized third-party access to portions of our North American network systems. We immediately brought in a top cybersecurity investigation firm and experienced legal counsel to conduct a comprehensive investigation. While Refresco was largely able to restore full functionality of its North American network and operations within a week, the investigation into what information was potentially compromised took much longer and involved a manual review of a large volume of data by an experienced and industry leading outside vendor.
>
> **What Information Was Involved?** At this time, based on the outside vendor's review, we believe that some personally identifiable information belonging to certain current or former Refresco employees and certain spouses and/or dependents of Refresco employees may have been impacted in the incident. In addition, we believe that some individuals' personal health information, as provided in connection with workers' compensation and/or ADA accommodations proceedings, may also have been impacted. The impacted personal information may include the categories listed on Attachment A. Although we have no evidence that any of your specific personal information was misused in any manner, this notification is being sent as part of the appropriate precautionary measures we are taking to protect your financial security and help alleviate concerns you may have.

39. Defendant's Notice Letter lists time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing two years of credit monitoring that Plaintiff and Class Members would have to affirmatively sign up for, and a call center number that victims may contact with questions, Defendant offered no other substantive steps to help victims like Plaintiff and Class Members protect themselves. On information and belief, Defendant sent a similar generic letter to all other individuals affected by the Data Breach.

40. Omitted from the Notice Letter were the dates of Defendant's investigation, the date the Defendant detected the data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, any explanation as to why it took Defendant more than seven months after the Data Breach to inform impacted individuals, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

41. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

42. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

43. 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, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

44. Defendant had obligation created by HIPAA, FTCA, industry standards, common law, and representations made to Plaintiff and Class members to keep their Private Information confidential and to protect it from unauthorized access

and disclosure.

45. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class members, including their name, date of birth, Social Security numbers, street address, financial account number, driver's license number, health insurance policy number, and certain health information as provided in connection with workers' compensation and/or ADA accommodations proceedings. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

PLAINTIFF BERRY'S EXPERIENCE

46. Plaintiff Berry was an employee of Cott Beverages before it was acquired by Defendant Refresco. Plaintiff's employment ran from December 2015 through February 2018.

47. In order to obtain medical coverage from Defendant, Plaintiff was required to provide his Private Information to Defendant.

48. At the time of the Data Breach—in March 2023—Refresco retained Plaintiff Berry's Private Information in its system.

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

50. Plaintiff Berry became aware of the Data Breach when he received a Data Breach notification letter in the mail, on or around November 15, 2023. Plaintiff immediately took steps to protect and vindicate his rights, including by maintaining a credit freeze on his accounts and by initiating this litigation. Due to the recency of his discovery, Plaintiff will be expending appreciable time and energy monitoring his accounts and remaining alert of fraud or identity theft attempts.

51. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Berry made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach as well as checking his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time remedying the breach—including by placing or maintaining credit freezes on his accounts– valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

52. As with all Class members, Plaintiff Berry has faced and will continue to face a certainly impending and substantial risk of future harms as a result of Defendant's completely lax and ineffectual data security measures, as further set forth herein. Some of these harms will include fraudulent charges, charges, loans or medical procedures ordered in class members' names without their permission, and targeted advertising without class members' consent.

53. Some of these harms may not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

54. Mr. Berry has already suffered hardship as a result of the Data Breach. On or around September 25, 2023, Plaintiff received a notification from Discover indicating that his Social Security number had been compromised and was found on the Dark Web.

55. As a result of the Data Breach including his compromised Social Security number, Plaintiff Berry purchased credit monitoring services on or around September 30, 2023, from myfico.com costing $39.95.

56. On or around December 6, 2023, Plaintiff received another notification from Discover indicating that his Social Security number had been compromised and was found on the Dark Web.

57. As a result of the Data Breach including his compromised Social Security number, Plaintiff Berry again purchased credit monitoring services on or around January 29, 2024 and February 28, 2024, from myfico.com each time costing $39.95.

58. Plaintiff suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time spent on activities

remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminution of value of his Private Information; (vi) the continued and increased risk of fraud and identity theft; (vii) and loss of the money Plaintiff spent on credit monitoring.

59. The Data Breach has caused Plaintiff Berry to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

60. As a result of the Data Breach, Plaintiff Berry anticipates spending, and has spent, considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Berry is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

A. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Employees' Private Information

62. Defendant acquires, collects, and stores a massive amount of its employees' Private Information, including health information and other personally identifiable data.

63. As a condition of employment, Defendant requires that these employees entrust them with highly confidential Private Information.

64. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and class members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and class members' Private Information from disclosure.

65. Defendant had obligations created by the Health Insurance Portability Act (42 U.S.C. § 1320d *et seq.*) ("HIPAA"), industry standards, common law, and representations made to class members, to keep class members' Private Information confidential and to protect it from unauthorized access and disclosure.

66. Defendant failed to properly safeguard class members' Private Information, allowing hackers to access their Private Information.

67. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

68. Before, during, and after the Data Breach, Defendant promised employees that their Private Information would be kept confidential.

69. Defendant's failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because Defendant operates in

a field which has recently been a frequent target of scammers attempting to fraudulently gain access to highly confidential Private Information.

70. In fact, Defendant has been on notice for years that collect Private Information are a prime target for scammers because of the amount of confidential customer information maintained.

71. Defendant was also on notice that the FBI has been concerned about data security of employers that collect and store healthcare information. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies that collect and store healthcare information that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[6]

72. The American Medical Association ("AMA") has also warned companies that collect and store healthcare information about the importance of protecting their employees' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also

[6] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare- firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

patient access to care.[7]

73. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[8] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[9] That trend continues.

74. When compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[10] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the

[7] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[8] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[9] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[10] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

economy as a whole.[11]

75. A 2017 study conducted by HIMSS Analytics showed that email was the most likely cause of a data breach, with 78 percent of providers stating that they experienced a healthcare ransomware or malware attack in the past 12 months.

76. Healthcare related data breaches continued to rapidly increase into 2023 when Defendant was breached.[12]

77. In various industries, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS).

78. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[13]

79. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

---

[11] *Id.*

[12] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

[13] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

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

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of

full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

80. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

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

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk,

search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[14]

[14] *See Security Tip (ST19-001) Protecting AgainstRansomware*, CYBERSECURITY

81. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**

& INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[15]

82. These are basic, common-sense email security measures. Defendant, with its heightened standard of care, should be doing even more. By taking these commercially reasonable, common-sense steps, Defendant could have prevented this Data Breach from occurring.

83. Charged with handling sensitive PII including healthcare information, Defendant knew, or should have known, the importance of safeguarding its employees' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant employees as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

84. The PII was also maintained on Defendant's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's systems through cyberattacks. The potential for cyberattacks and the resultant

[15] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/

improper disclosure of Plaintiffs' and class members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

B. The Monetary Value of Privacy Protections and Private Information

85. The fact that Plaintiff's and Class Members' Private Information was stolen—and is likely presently offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

86. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

87. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[16] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive health information on multiple underground Internet websites, commonly referred to as the dark web.

88. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records,

[16] Federal Trade Commission, *Warning Signs of IdentityTheft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

> information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[17]

89. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[18]

90. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[19]

91. Recognizing the high value that consumers place on their Private

---

[17] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace- merging-and-exchanging-consumer-data/transcript.pdf.

[18] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

[19] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

Information, many companies now offer consumers an opportunity to sell this information.[20] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

92. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[21]

93. The value of Plaintiff's and Class Members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[22] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims,

[20] *Web's Hot New Commodity*, *supra* note 17

[21] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[22] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

94. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[23]

95. The ramifications of Defendant's failure to keep its employees' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

96. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[24] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of

[23] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.

[24] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[25]

97. When compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[26] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[27]

98. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and

[25] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[26] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

[27] *Id.*

could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting related industries.

99. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the cyberattack into its systems and, ultimately, the theft of its employees' Private Information.

100. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[28] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[29] Based upon information and belief, the unauthorized parties utilized the Private

[28] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer- privacy-era-rapid-change-proposed-framework.

[29] *See Id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class Members that was misused.

101. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

102. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

103. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

C. Defendant's Conduct violated HIPAA

104. HIPAA requires covered entities like Defendant protect against reasonably anticipated threats to the security of PHI. Covered entities must

implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[30]

105. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

106. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[31]

107. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Defendant's security failures include, but are not limited to, the following:

- Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation

[30] *What is Considered Protected Health Information Under HIPAA*?, HIPAA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

[31] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

of 45 C.F.R. §164.306(a)(1);

- Failing to implement 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 in violation of 45 C.F.R. §164.312(a)(1);

- Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

- Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

- Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

- Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

- Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

- Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

- Failing to effectively train all members of their

workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

- Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

108. The FTC has promulgated numerous guides for businesses that 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.[32]

109. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[33] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

[32] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[33] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

110. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private 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.[34]

111. 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.

112. Defendant was at all times fully aware of its obligation to protect the Private Information of employees because of its position as a trusted healthcare provider. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Defendant Failed to Comply with Healthcare Industry Standards

113. HHS's Office for Civil Rights has stated:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their

[34] *Start with Security*, *supra* note 32

> systems and data, this is especially important in the healthcare industry.
>
> Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[35]

114. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) properly encrypting Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

115. Private cybersecurity firms have also promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.[36]

116. Despite the abundance and availability of information regarding cybersecurity best practices, Defendant chose to ignore them. These best practices were known, or should have been known by Defendant, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

---

[35] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare- organizations/.

[36] [36]*See, e.g.*, *10 Best Practices For Healthcare Security*, INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.

E. Damages to Plaintiff and the Class

117. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

118. The ramifications of Defendant's failure to keep employees' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Victims of data breaches are more likely to become victims of identity fraud.[37]

119. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

120. Defendant further owed and breached its duty to Plaintiff and Class Members to notify past and present employees affected by the Data Breach in a timely manner.

121. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able

[37] *2014 LexisNexis True Cost of FraudStudy*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse of Plaintiff's and Class Members' Private Information as detailed above, and Plaintiff is now at a heightened and increased risk of identity theft and fraud.

122. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Victims of identity theft may lose out on job opportunities, or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

123. Some of the risks associated with the loss of personal information have already manifested themselves in Plaintiff's case. Defendant's Notice Letter advises employees like Mr. Berry about the release of sensitive Private Information and that he should remain vigilant of fraudulent activity on his accounts, with no other explanation of where this information could have gone, or who might have access to it.

124. Plaintiff and Class Members have suffered or face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, medical services billed in their name, and similar identity theft.

125. Plaintiff and Class Members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit

report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

126. Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received "benefits" that were of a diminished value to that described in their agreements with Defendant. They were damaged in an amount at least equal to the difference in the value of the healthcare coverage with data security protection they paid for and the coverage they received.

127. Plaintiff and Class Members would not have obtained coverage from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

128. Plaintiff and Class Members will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

129. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[38] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use

[38] *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[39] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[40]

130. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[41]

131. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the healthcare industry context, Private Information can be used to submit false insurance claims. As a result, Plaintiff and Class Members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and

[39] *Id.*

[40] *Id.*

[41] *Id.*

will need to monitor their credit for an indefinite duration. For Plaintiff and Class Members, this risk creates unending feelings of fear and annoyance. Private Information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

132. As a result of the Data Breach, Plaintiff and Class Members' Private Information has diminished in value.

133. The Private Information belonging to Plaintiff and Class Members is private and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiff and Class Members that was of an extremely personal, sensitive nature as a direct result of its inadequate security measures.

134. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or

integrity of such information.

135. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

136. Defendant did not properly train their employees to identify and avoid cyberattacks.

137. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

138. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and 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 the actual and potential impact of the Data Breach on their lives.

139. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the

problems caused by identity theft [could] take more than a year for some victims."[42]

140. Other than offering 24 months of credit monitoring, Defendant took no measures to assist Plaintiff and Class Members, other than suggesting some potential ways they might check their own accounts for fraud. None of these recommendations, however, would require Defendant to expend any effort to protect Plaintiff's and Class Members' Private Information.

141. Defendant's failure to adequately protect Plaintiff's and Class Members' Private Information has resulted in them having to undertake these tasks themselves, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Defendant's Data Breach Notice indicates, it is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

142. While Defendant offered some complimentary credit monitoring, Plaintiffs could not trust a company that had already breached his data. The credit monitoring offered from TransUnion does not guarantee privacy or data security for Plaintiff, who would have to expose his information once more to get monitoring services. Thus, to mitigate harm, Plaintiff and Class Members are now burdened

[42] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

with indefinite monitoring and vigilance of their accounts.

143. Moreover, the offer of 24 months of identity monitoring to Plaintiff and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is *acquired* by criminals and when it is *used* by them. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[43] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

144. Plaintiff and Class Members have been damaged in several other ways as well. Plaintiff and Class Members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class Members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Class Members have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing

[43] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not- beworth-the-cost.html

fraudulent or suspicious activity on their accounts. Plaintiff and Class Members also suffered a loss of the inherent value of their Private Information.

145. The Private Information stolen in the Data Breach can be misused on its own, or it can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the target might agree to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

146. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;

- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

- Anxiety and distress resulting fear of misuse of their Private Information.

147. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

148. Plaintiff brings this action individually and on behalf of the following nationwide class pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(2), and/or 23(b)(3). Specifically, the nationwide class consists of the following:

> **Nationwide Class:**
> All persons whose Private Information was compromised as a result of the Data Breach discovered on or about May 14, 2023, and who were sent notice of the Data Breach.

149. In the alternative to the Nationwide Class, and pursuant to Federal Rule of Civil Procedure 23(c)(5), Plaintiff Berry seeks to represent the following state subclass with respect to Counts Five, Six, and Seven in the event that the Court

declines to certify the Nationwide Class above, as well as with respect to the California state law claims regardless of certification of the Nationwide Class:

> **California Subclass:**
> All persons in California whose Private Information was compromised as a result of the Data Breach discovered on or about May 14, 2023, and who were sent notice of the Data Breach.

150. The Nationwide Class and the California Subclass are referred to herein as the "Class."

151. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any such entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

152. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

153. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his 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.

154. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The

members of the class are so numerous that joinder of all class members would be impracticable. On information and belief, the Nationwide Class numbers in the hundreds of thousands. The Defendant itself reported that more than 25,170 people were affected by its Data Breach.

155. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiff and the Class's Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures

designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;

- Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;
- Whether Defendant was negligent in failing to timely notify Plaintiff and the Class of the Data breach;
- Whether Defendant was unjustly enriched by its actions; and
- Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

156. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other members of the Class. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

157. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class Members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to

Plaintiff.

158. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because his interests do not conflict with the interests of the Class she seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

159. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

160. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** 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 or other financial detriment suffered by Plaintiff and the other members of the Class 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 members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class 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 a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On Behalf of Plaintiff and All Class Members)

161. Plaintiff repeats and realleges paragraphs 1 through 147 as though fully set forth herein.

162. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as such.

163. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

164. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private

Information in their possession;

- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

165. Defendant also breached its duty to Plaintiff and Class Members to adequately protect and safeguard Private Information, and to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse. This permitted a malicious third party to gather Plaintiff's and Class Members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

166. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

167. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' Private Information.

168. 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.

169. Because Defendant knew that a breach of its systems would damage thousands of its employees, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

170. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

171. 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.

172. Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about an employee that—if it were to fall into the wrong hands—could

present a risk of harm to the employee's finances or reputation.

173. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

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

- Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;
- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Plaintiff's and Class Members' Private Information; and
- 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

175. Through Defendant's acts and omissions described in this Complaint, Defendant breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' Private Information during the time it was within

Defendant's possession or control.

176. Defendant's conduct was grossly negligent and departed from all reasonable standards of care.

177. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

178. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class Members suffered damages as alleged above.

179. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all class members.

COUNT II
Breach of Contract
(On Behalf of Plaintiff and All class members)

180. Plaintiff repeats and realleges paragraphs 1 through 147 as though fully set forth herein.

181. Plaintiff and other Class Members entered into valid and enforceable express contracts with Defendant under which Plaintiff and other Class Members agreed to provide their Private Information to Defendant, and Defendant agreed to

provide healthcare coverage and, impliedly, if not explicitly, agreed to protect Plaintiff's and Class Members' Private Information.

182. These contracts include HIPAA privacy notices and explanation of benefits documents.

183. To the extent Defendant's obligation to protect Plaintiff's and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and other Class Members' Private Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. No Plaintiff would have entered into these contracts with Defendant without understanding that Plaintiff's and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

184. A meeting of the minds occurred, as Plaintiff and other Class Members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

185. The protection of Plaintiff's and Class Members' Private Information were material aspects of Plaintiff's and Class Members' contracts with Defendant.

186. Defendant's promises and representations described above relating to

HIPAA and industry practices, and about Defendant's purported concern about their clients' privacy rights, became terms of the contracts between Defendant and their clients, including Plaintiff and other class members. Defendant breached these promises by failing to comply with HIPAA and reasonable industry practices.

187. Plaintiff and Class Members read, reviewed, and/or relied on statements made by or provided by Defendant and/or otherwise understood that Defendant would protect its employees' Private Information if that information were provided to Defendant.

188. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant. Defendant did not.

189. As a result of Defendant's breach of these terms, Plaintiff and other Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health coverage Defendant promised and the insecure coverage received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiff and other Class Members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private

Information, which may take years to manifest, discover, and detect.

190. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members, in the Alternative to Count II)

191. Plaintiff repeats and realleges paragraphs 1 through 147 as though fully set forth herein.

192. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of healthcare coverage, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

193. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when he first entered into the employment agreement with Defendant.

194. The valid and enforceable implied contracts to provide medical coverage that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or

that Defendant creates on its own from disclosure.

195. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's medical coverage, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

196. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

197. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

198. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

199. Under implied contracts, Defendant promised and was obligated to: (a) provide medical coverage to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiff and Class Members agreed to pay money for these services, and to turn over their Private Information.

200. Both the provision of medical coverage and the protection of Plaintiff's

and Class Members' Private Information were material aspects of these implied contracts.

201. The implied contracts for the provision of medical coverage—contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including, on information and belief, Defendant's employment contract and Data Breach notification letter.

202. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and protect the privacy of Plaintiff's and Class Members' Private Information.

203. Defendant's current and former employees value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining legitimate medical coverage. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected. Nor would they have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

204. A meeting of the minds occurred, as Plaintiff and Class Members agreed and provided their Private Information to Defendant and/or its affiliated healthcare partners, and paid for the provided medical coverage in exchange for, amongst other things, both the provision of healthcare and the protection of their Private Information.

205. Plaintiff and Class Members performed their obligations under the contract when they paid for Defendant's coverage and provided their Private Information.

206. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

207. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notifications of the Data Breach. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class Members' Private Information as set forth above.

208. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

209. As a result of Defendant's failure to fulfill the data security protections

promised in these contracts, Plaintiff and Class Members did not receive full benefit of the bargain, and instead received healthcare coverage and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare coverage with data security protection they paid for and the healthcare coverage they received.

210. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class Members, nor any reasonable person would have obtained healthcare from Defendant and/or its affiliated partners.

211. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

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

213. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its 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
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All Class Members)

214. Plaintiff repeats and realleges paragraphs 1 through 147 as though fully set forth herein.

215. In providing their Private Information to Defendant, Plaintiff and Class Members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and Class Members to safeguard and keep confidential that Private Information.

216. Defendant accepted the special confidence Plaintiff and Class Members placed in it, as evidenced by its assertion that it takes its "responsibilities to protect your personal information very seriously[,]" as included in the Data Breach Notice Letter.

217. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and Class Members for the safeguarding of Plaintiff's and Class Member's Private Information.

218. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its employees' relationship, in particular, to keep secure the Private Information of its employees.

219. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

220. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

221. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains 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 its continued possession; (vi) future costs in terms of time, effort, and money that will

be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

222. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Violation of the California Constitution's Right to Privacy
(Cal. Const., art. I, § 1)
(By Plaintiff Berry on Behalf of the California Subclass)

223. Plaintiff repeats and realleges paragraphs 1 through 147 as though fully set forth herein. The California Constitution provides:

> "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy." (Cal. Const., art. I. § 1.)

224. Plaintiff and the California Subclass have a legally recognized and protected privacy interest in the Private Information provided to and obtained by Defendant, including but not limited to, an interest in precluding the dissemination or misuse of this sensitive and confidential information and the misuse of this information for malicious purposes.

225. Plaintiff and the Subclass reasonably expected Defendant would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their Private Information and the substantial, imminent risk of the

unauthorized use thereof.

226. Defendant's conduct described herein resulted in a serious invasion of privacy of Plaintiff and the Subclass, as the release of Private Information could highly offend a reasonable individual.

227. As a direct consequence of the actions as identified above, Plaintiff and California Subclass members suffered harms and losses, including but not limited to, the loss of control over use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation and attempt to cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of imminent future loss, and privacy injuries associated with having their sensitive Private Information disclosed.

COUNT VI
Violation of Florida's Deceptive and Unfair Practices Act ("FDUPTA")
Fla. Stat. § 501.201 *et seq.*
(On Behalf of Plaintiff and All Class Members)

228. Plaintiff repeats and realleges paragraphs 1 through 147 as though fully set forth herein.

229. Plaintiff, Class Members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") Fla. Stat. § 501.201, *et seq.*

230. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of

FDUTPA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach; Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Private Information; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

231. Defendant's representations and omissions were material because they were likely to deceive reasonable former and current employees about the adequacy of Defendant's data security and ability to protect the confidentiality of employees' Private Information.

232. In addition, Defendant's failure to secure employees' PHI violated the

FTCA and HIPAA, and therefore violated the FDUPTA *per se*.

233. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

234. The aforesaid conduct constitutes a violation of FDUTPA, Fla. Stat. § 501.204, in that it is a restraint on trade or commerce.

235. The Defendant's violations of FDUPTA have an impact of great and general importance on the public, including Floridians. Thousands of Floridians have been employed by Defendant, many of whom have been impacted by the Data Breach. In addition, Florida residents have a strong interest in regulating the conduct of its corporate citizens such as Defendant, whose policies and practices described herein affected thousands across the country.

236. As a direct and proximate result of Defendant's violation of FDUPTA, Plaintiff and Class Members are entitled to judgment under Fla. Stat. § 501.201, *et seq*, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

237. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and other Class Members' Private Information constitute representations as to characteristics, uses or benefits of services that such

services did not actually have, in violation of Fla. Stat. § 501.202(2).

238. On information and belief, Defendant formulated and conceived of the systems it used to compile and maintain employee information largely within the state of Florida, oversaw its data privacy program complained of herein from Florida, and its communications and other efforts to hold employee data largely emanated from Florida.

239. Most, if not all, of the alleged misrepresentations and omissions by Defendant complained of herein that led to inadequate safety measures to protect employee information occurred within or were approved within Florida.

240. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and Class Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Fla. Stat. § 501.204.

241. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant advertised it is committed to protecting privacy and securely maintaining personal information. Defendant did not securely maintain personal information as represented, in violation of Fla. Stat. § 501.171.

242. These violations have caused financial injury to Plaintiff and Class

Members and have created an unreasonable, imminent risk of future injury.

243. Accordingly, Plaintiff, on behalf of himself and the other Class Members, brings this action under the Deceptive and Unfair Trade Practices Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT VII
Declaratory Relief
(On Behalf of Plaintiff and All class members)

244. Plaintiff repeats and realleges paragraphs 1 through 147 as though fully set forth herein.

245. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

246. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further

compromises their Private Information will occur in the future.

247. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' Private Information.

248. Defendant still possesses the Private Information of Plaintiff and the Class.

249. Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

250. Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

251. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial.

252. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs to Defendant, Plaintiff and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and

Defendant has a pre-existing legal obligation to employ such measures.

253. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach to Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class Members, along with other consumers whose Personal Information would be further compromised.

254. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant owed and continues to owe a duty to implement and maintain reasonable security measures, including but not limited to the following:

- Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- engaging third-party security auditors and internal personnel to run automated security monitoring;
- auditing, testing, and training its security personnel regarding any new or modified procedures;
- purging, deleting, and destroying Private Information not necessary for

its provisions of employment in a reasonably secure manner;

- conducting regular database scans and security checks; and
- routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the classes;

B. For equitable relief enjoining Defendant from engaging in the conduct complained herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For declaratory relief concluding that that Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the Private Information with which it is entrusted, specifically including information pertaining to healthcare and financial records it

obtains from its clients, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act.

D. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than three (3) years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, treble damages, and statutory penalties, in the amount to be determined by allowable law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expenses, including expert witnesses fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this Court may deem just and proper.

Dated: February 14, 2024

Respectfully Submitted.

/s/ *Scott D. Hirsch*
Scott D. Hirsch
SCOTT HIRSCH LAW GROUP, PLLC
Fla. Bar No. 50833
6810 N. State Road 7
Coconut Creek, FL 33073
Tel: (561) 569-7062
Email: scott@scotthirschlawgroup.com

MIGLIACCIO & RATHOD LLP
Nicholas A. Migliaccio, Esq.*
Jason S. Rathod, Esq.*
412 H Street N.E., Suite 302
Washington, D.C. 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
* Pro hac vice admission to be sought

Attorneys for Plaintiff and the putative class

ClassAction.org