UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

In re: Berry, Dunn, McNeil & Parker Data Security Incident Litigation	Lead Case No. 2:24-cv-00146 **DEMAND FOR JURY TRIAL**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Quinton Anderson, Michael Meyerson, Laura Russell, Kathy Bishop, Randy Bishop, Kristie Iushkova, Robert Hickman, Sally Hughes, Donald Dee Smith, Melody Bowman, Brandy Brady, Virginia Demel-Duff, Myron Nottingham, Yasmine Encarnacion, and Tonya Gambino (collectively, "Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendants Berry, Dunn, McNeil & Parker, LLC ("Berry Dunn") and ZZ Enterprises, LLC d/b/a Reliable Networks of Maine, LLC ("Reliable Networks," and collectively with Berry Dunn, "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated individuals' personally identifiable information ("PII") and protected health information ("PHI" and together with PII, "Private Information") from criminal hackers.

2. Berry Dunn, based in Portland, Maine, is a national consulting and accounting firm that serves a variety of businesses and governmental entities, as well as individual clients.

3. Reliable Networks, based in Biddeford, Maine, is a technology consulting company that offers services to its customers, including but not limited to, cloud hosting, managed services, IT consulting and security.

4. Berry Dunn's Health Analytics Practice Group ("HAPG") contracted with Reliable Networks as a managed service provider.

5. On or about April 25, 2024, Berry Dunn filed official notice of a hacking incident with the Office of Maine Attorney General.[1] Under state and federal law, organizations must report breaches involving PHI within at least 60 days.

6. On or around the same time, Berry Dunn also sent out data breach notice letters ("Notice Letter") to individuals whose information was compromised as a result of the hacking incident.

7. Based on the Notice Letter sent to Plaintiffs and "Class Members" (defined below), unusual activity was detected on Reliable Networks' systems on September 14, 2023. In response, Berry Dunn launched an investigation, which revealed that an unauthorized party had access to certain files that contained sensitive information related to Berry Dunn's HAPG, which manages its clients' and their patients' data, and that such access took place on an undisclosed date (the "Data Breach"). Yet, Berry Dunn waited seven months to notify the public that they were at risk.

8. As a result of this delayed response, Plaintiffs and Class Members had no idea for seven months that their 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. This risk will remain for their respective lifetimes.

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/f51173b0-8935-424e-871a-08e64c147b2e.shtml (last visited June 18, 2024).

9. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, Social Security numbers, dates of birth, and individual health insurance policy numbers that Berry Dunn collected and maintained.

10. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns and insurance claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. There has been no assurance offered by Defendants that all of Class Members' Private Information or copies thereof have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficient to avoid a similar breach of their network in the future.

12. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

13. Plaintiffs bring this class action lawsuit to address Defendants' inadequate safeguarding of Class Members' Private Information that Berry Dunn collected and maintained,

and their failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

14. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure the Private Information left them vulnerable to an attack.

15. Upon information and belief, Berry Dunn failed to properly monitor its vendor, Reliable Networks, and the computer network and systems that housed the Private Information. Had Berry Dunn properly monitored its vendor and implemented its own proper data security and monitoring protocols, it could have prevented the Data Breach or at least discovered it and alerted Plaintiffs and Class Members thereof sooner.

16. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct as the Private Information that Defendants collected, maintained, and transferred is now in the hands of data thieves and other unauthorized third parties.

17. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

II. PARTIES

18. Plaintiff Quinton Anderson is and at all times mentioned herein was an individual citizen of the Commonwealth of Pennsylvania.

19. Plaintiff Michael Meyerson is and at all times mentioned herein was an individual citizen of the Commonwealth of Pennsylvania.

20. Plaintiff Laura Russel is and at all times mentioned herein was an individual citizen of the State of West Virginia.

21. Plaintiff Randy Bishop is and at all times mentioned herein was an individual citizen of the State of West Virginia.

22. Plaintiff Kathy Bishop is and at all times mentioned herein was an individual citizen of the State of West Virginia.

23. Plaintiff Kristie Iushkova is and at all times mentioned herein was an individual citizen of the Commonwealth of Pennsylvania.

24. Plaintiff Robert Hickman is and at all times mentioned herein was an individual citizen of the State of West Virginia.

25. Plaintiff Sally Hughes is and at all times mentioned herein was an individual citizen of the Commonwealth of Pennsylvania.

26. Plaintiff Donald Dee Smith is and at all times mentioned herein was an individual citizen of the State of Ohio.

27. Plaintiff Melody Bowman is and at all times mentioned herein was an individual citizen of the State of West Virginia.

28. Plaintiff Brandy Brady is and at all times mentioned herein was an individual citizen of the State of North Carolina.

29. Plaintiff Virginia Demel-Duff is and at all times mentioned herein was an individual citizen of the Commonwealth of Pennsylvania.

30. Plaintiff Myron Nottingham is and at all times mentioned herein was an individual citizen of the State of West Virginia.

31. Plaintiff Yasmine Encarnacion is and at all times mentioned herein was an individual citizen of the Commonwealth of Pennsylvania.

32. Plaintiff Tonya Gambino is and at all times mentioned herein was an individual citizen of the Commonwealth of Pennsylvania.

33. Defendant Berry Dunn is a consulting and accounting firm with its principal place of business at 2211 Congress Street, Portland, Maine, 04102.

34. Defendant Reliable Networks is a limited liability company organized under the laws of Maine and with a principal place of business at 6 Shepherds Way, Biddeford, Maine 04005.

III. JURISDICTION AND VENUE

35. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

36. This Court has jurisdiction over Defendants because Defendants operate in and/or are incorporated in this District.

37. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Defendants have harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Defendants' Business and Collection of Plaintiffs' and Class Members' Private Information

38. Berry Dunn is a leading national professional services firm providing assurance, tax, and consulting services to businesses, nonprofits, individuals, and government agencies

throughout the US and its territories.[2] Founded in 1974, Berry Dunn provides these services across a broad array of industries and business sectors, including hospitals and healthcare organizations. Through its business clients, Berry Dunn serves over a million individuals throughout the United States. Berry Dunn employs more than 200 people and generates approximately $43.5 million in annual revenue.

39. Reliable Networks is a provider of IT services and IT advising to its customers, including Berry Dunn.[3]

40. As a condition of receiving services, Berry Dunn requires that its clients entrust it with their patients' highly sensitive personal and health information, including the Private Information compromised in the Data Breach. Plaintiffs and Class Members were thus required to provide their Private Information to Defendants.

41. In turn, Berry Dunn negligently stored and maintained Plaintiffs' and Class Members' Private Information on Reliable Networks' vulnerable, and unsecured systems.[4]

42. In its Privacy Policy, Berry Dunn promises its clients and their patients that "we endeavor to protect such information against unauthorized disclosures by using secure technologies. Berry Dunn uses reasonable safeguards designed to protect your information through our databases, policies, and procedures. We also take reasonable steps to ensure that our service providers also protect our information."[5]

43. Thus, due to the highly sensitive and personal nature of the information Defendants acquire and store with respect to their clients' patients, Defendants, upon information and belief,

---

[2] *See* https://www.berrydunn.com/about (last visited Apr. 29, 2024).
[3] *See* https://www.reliablenetworks.com/about/ (last visited June 7, 2024).
[4] *See* https://www.berrydunn.com/notice-of-reliable-networks-security-incident (last visited June 7, 2024).
[5] *See* https://www.berrydunn.com/privacypolicy.aspx (last visited Apr. 24, 2024).

promise to, among other things: keep individuals' Private Information private; comply with industry standards related to data security and the maintenance of its clients' patients' Private Information; inform its clients' patients of its legal duties relating to data security and comply with all federal and state laws protecting their Private Information; only use and release individuals' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

44. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties they owed to them and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

45. Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendants ultimately failed to do.

B. The Data Breach and Defendants' Inadequate Notice to Plaintiffs and Class Members

46. According to Berry Dunn's Notice Letter, it learned of unauthorized access to Reliable Networks' computer systems on September 14, 2023, with such unauthorized access having taken place on an undisclosed date.

47. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including Social Security numbers and health insurance policy numbers.

48. On or about April 25, 2024, roughly seven months after Defendants learned that the Class's Private Information was first accessed by cybercriminals, Berry Dunn finally began to

notify its clients' patients that its investigation determined that their Private Information was affected. Reliable Networks provided no such notice.

49. Defendants had obligations created by contract, industry standards, common law, and its own representations to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure. They failed to fulfill these obligations.

50. Plaintiffs and Class Members allowed their Private Information to be entrusted to Berry Dunn and Reliable Networks with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

51. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

52. Defendants knew or should have known that its electronic records whereon Plaintiffs' and Class Members' Private Information was being stored would be targeted by cybercriminals.

C. The Healthcare Sector Is Particularly Susceptible to Data Breaches.

53. Defendants were on notice that companies in the healthcare industry are susceptible targets for data breaches.

54. Defendants were also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry 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 (PHI)."[6]

55. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting patients' 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 patient access to care.[7]

56. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[8] In 2022, the largest growth in compromises occurred in the healthcare sector.[9]

57. Indeed, 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]

---

[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-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Apr. 29, 2024).
[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 (last visited Apr. 29, 2024)
[8] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report,* https://www.idtheftcenter.org/2018-data-breaches/ (last visited Apr. 29, 2024).
[9] Identity Theft Resource Center, *2022 End-of-Year Data Breach Report,* https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited Apr. 29, 2024).
[10] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited Apr. 29, 2024).

58. 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 economy as a whole.[11]

59. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[12]

60. Defendants knew, or should have known, the importance of safeguarding patients' Private Information, including PHI, entrusted to them, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Defendants' clients' patients as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Defendants Failed to Comply with FTC Guidelines.

61. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision

[11] *Id*.
[12] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Apr. 4, 2019, https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Apr. 29, 2024).

making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

62. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. 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. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

65. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

66. Defendants were, at all times, fully aware of their obligation to protect the Private Information belonging to Plaintiffs and Class Members, yet they failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

E. Defendants Failed to Comply with Industry Standards.

67. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

68. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Defendants include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

69. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training

staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

70. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

71. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

F. Defendants Breached their Duty to Safeguard Plaintiffs' and Class Members' Private Information.

72. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Private Information of Class Members.

73. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect their clients' patients' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to sufficiently train their employees regarding the proper handling of their clients' patients' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA; and

f. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

74. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access their computer network and systems which contained unsecured and unencrypted Private Information.

75. Had Defendants remedied the deficiencies in their information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

76. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendants.

G. Defendants Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft.

77. The FTC hosted a workshop to discuss "informational injuries," which are injuries that individuals, like Plaintiffs and Class Members, suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[13] Exposure of highly sensitive personal information that an individual wishes to keep private may cause harm to that individual, such as the ability to obtain or keep employment. A loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

78. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

79. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired

[13] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* FED. TRADE COMM'N (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited Apr. 29, 2024).

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

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

81. Thus, even if certain information were not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

82. One such example of this is the development of "Fullz" packages.

83. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

84. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such

as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

85. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[14] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

86. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[14] *See IdentityTheft.gov,* FED. TRADE COMM'N, https://www.identitytheft.gov/Steps (last visited Apr. 29, 2024).

87. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[15]

88. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

89. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[16]

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

91. Medical identity 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."[17]

---

[15] Federal Trade Commission, *Warning Signs of Identity Theft,* https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Apr. 29, 2024).
[16] Center for Internet Security, *Data Breaches: In the Healthcare Sector,* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited Apr. 29, 2024).
[17] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," KAISER HEALTH NEWS (Feb. 7, 2014), https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited Apr. 29, 2024).

92. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

93. Here, not only was sensitive medical insurance information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

94. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[18]

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

95. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

[18] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), https://www.gao.gov/assets/270/262904.html (last visited Apr. 29, 2024).

96. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. Plaintiffs' and Class Members' Experiences

Plaintiff Quinton Anderson's Experience

97. Plaintiff Anderson received a Notice Letter from Berry Dunn dated April 25, 2024, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

98. Plaintiff Anderson is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

99. Plaintiff Anderson stores any documents containing his Private Information in a safe and secure location. Anderson has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

100. Because of the Data Breach, Plaintiff Anderson's Private Information is now in the hands of cyber criminals.

101. Plaintiff Anderson has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

102. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and PHI, Plaintiff Anderson is now subject to a present and continuing risk of crippling identity theft and fraud for his lifetime.

103. Since the Data Breach, Plaintiff Anderson has experienced identity theft in the form of unauthorized charges on credit and debit cards which caused Plaintiff Anderson to replace two cards. Plaintiff Anderson has also experienced a substantial increase in spam and phishing phone

calls, text messages, and emails. Plaintiff Anderson attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he has never experienced anything like this prior to now, and, to his knowledge, his Private Information has never been exposed in any other Data Breach.

104. As a result of the Data Breach, Plaintiff Anderson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Anderson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

105. The Notice Letter Plaintiff Anderson received from Berry Dunn specifically directed him to take the actions described above. Indeed, the Notice Letter advised Plaintiff and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[19] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[20] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on

[19] *See* Sample Notice Letter, https://apps.web.maine.gov/online/aeviewer/ME/40/f51173b0-8935-424e-871a-08e64c147b2e.shtml.
[20] *Id.*

credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[21]

106. As a result of the Data Breach, Plaintiff Anderson has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Anderson fears that criminals will use his information to commit identity theft.

107. Plaintiff Anderson anticipates spending considerable time and money on an ongoing basis.

108. Plaintiff Anderson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and continuing risk of injury flowing from fraud and identity theft posed by Plaintiff Anderson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Anderson's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Anderson's Private Information; and (e) continued risk to Plaintiff Anderson's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

[21] *Id.*

Plaintiff Michael Meyerson's Experience

109. Plaintiff Meyerson received a Notice Letter from Berry Dunn dated April 25, 2024, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

110. Plaintiff Meyerson is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

111. Plaintiff Meyerson stores any documents containing his Private Information in a safe and secure location. Plaintiff Meyerson has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

112. Because of the Data Breach, Plaintiff Meyerson's Private Information is now in the hands of cyber criminals.

113. Plaintiff Meyerson has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

114. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and PHI, Plaintiff Meyerson is now subject to a present and continuing risk of crippling identity theft and fraud for his lifetime.

115. As a result of the Data Breach, Plaintiff Meyerson has received extensive spam phone calls and emails. Plaintiff Meyerson did not receive these spam calls and emails prior to the Data Breach.

116. As a result of the Data Breach, Plaintiff Meyerson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Meyerson has already expended time and suffered loss of productivity from taking time to address and attempt to

ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

117. The Notice Letter Plaintiff Meyerson received from Berry Dunn specifically directed him to take the actions described above. Indeed, the Notice Letter advised Plaintiff and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[22] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[23] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[24]

118. As a result of the Data Breach, Plaintiff Meyerson has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Meyerson fears that criminals will use his information to commit identity theft.

119. Plaintiff Meyerson anticipates spending considerable time and money on an ongoing basis.

120. Plaintiff Meyerson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and

[22] *See* Sample Notice Letter at n.19, *supra*.
[23] *Id.*
[24] *Id.*

continuing risk of injury flowing from fraud and identity theft posed by Plaintiff Meyerson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Meyerson's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Meyerson's Private Information; and (e) continued risk to Plaintiff Meyerson's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Laura Russell's Experience

121. Plaintiff Russell received a Notice Letter from Berry Dunn dated April 25, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

122. Plaintiff Russell is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

123. Plaintiff Russell stores any documents containing her Private Information in a safe and secure location. Russell has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

124. Because of the Data Breach, Plaintiff Russell's Private Information is now in the hands of cyber criminals.

125. Plaintiff Russell has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

126. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number and PHI, Plaintiff Russell is now subject to a present and continuing risk of crippling identity theft and fraud for her lifetime.

127. Since the Data Breach, Plaintiff Russell has experienced identity theft in the form of an unauthorized charge on her debit card that caused her to request a new card. Plaintiff Russell has also experienced a substantial increase in spam and phishing phone calls. Plaintiff Russell attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never experienced anything like this prior to now, and, to her knowledge, her Private Information has never been exposed in any other Data Breach.

128. As a result of the Data Breach, Plaintiff Russell has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Russell has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

129. The Notice Letter Plaintiff Russell received from Berry Dunn specifically directed her to take the actions described above. Indeed, the Notice Letter advised Plaintiff and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[25] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[26] In

[25] *See* Sample Notice Letter at n.19, *supra*.
[26] *Id.*

addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[27]

130. As a result of the Data Breach, Plaintiff Russell has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Russell fears that criminals will use her information to commit identity theft.

131. Plaintiff Russell anticipates spending considerable time and money on an ongoing basis.

132. Plaintiff Russell has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and continuing risk of impending injury flowing from fraud and identity theft posed by Plaintiff Russell's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Russell's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Russell's Private Information; and (e) continued risk to Plaintiff Russell's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

[27] *Id.*

Plaintiff Randy Bishop's Experience

133. Plaintiff Randy Bishop received a Notice Letter from Berry Dunn dated April 25, 2024, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

134. Plaintiff Randy Bishop is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

135. Plaintiff Randy Bishop stores any documents containing his Private Information in a safe and secure location. Plaintiff Randy Bishop has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

136. Because of the Data Breach, Plaintiff Randy Bishop's Private Information is now in the hands of cyber criminals.

137. Plaintiff Randy Bishop has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

138. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and PHI, Plaintiff Randy Bishop is now subject to a present and continuing risk of crippling identity theft and fraud for his lifetime.

139. Since the Data Breach, Plaintiff Randy Bishop has experienced identity theft in the form of attempted Medicare fraud. An unknown person tried to use Plaintiff Randy Bishop's Medicare number to obtain medical services, which caused Plaintiff Bishop to request a new Medicare number. Plaintiff Bishop has also experienced unauthorized charges on his credit card and a substantial increase in spam and phishing phone calls. Plaintiff Randy Bishop attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the

fact that he has never experienced anything like this prior to now, and, to his knowledge, his Private Information has never been exposed in any other Data Breach.

140. As a result of the Data Breach, Plaintiff Randy Bishop has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Randy Bishop has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

141. The Notice Letter Plaintiff Randy Bishop received from Berry Dunn specifically directed him to take the actions described above. Indeed, the Notice Letter advised Plaintiff and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[28] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[29] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[30]

142. As a result of the Data Breach, Plaintiff Randy Bishop has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals

[28] *See* Sample Notice Letter at n.19, *supra*.
[29] *Id.*
[30] *Id.*

accessing and misusing his Private Information. Plaintiff Randy Bishop fears that criminals will use his information to commit identity theft.

143. Plaintiff Randy Bishop anticipates spending considerable time and money on an ongoing basis.

144. Plaintiff Randy Bishop has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and continuing risk of injury flowing from fraud and identity theft posed by Plaintiff Bishop's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Bishop's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Bishop's Private Information; and (e) continued risk to Plaintiff Randy Bishop's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Kristie Iushkova's Experience

145. Plaintiff Iushkova received a Notice Letter from Berry Dunn dated April 25, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

146. Plaintiff Iushkova is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

147. Plaintiff Iushkova stores any documents containing her Private Information in a safe and secure location. Plaintiff Iushkova has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

148. Because of the Data Breach, Plaintiff Iushkova's Private Information is now in the hands of cyber criminals.

149. Plaintiff Iushkova has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

150. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number and PHI, Plaintiff Iushkova is now subject to a present and continuing risk of crippling identity theft and fraud for her lifetime.

151. Since the Data Breach, Plaintiff Iushkova has experienced identity theft in the form of a substantial increase in spam and phishing calls, texts, and emails. Plaintiff Iushkova attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never experienced anything like this prior to now, and, to her knowledge, her Private Information has never been exposed in any other Data Breach.

152. As a result of the Data Breach, Plaintiff Iushkova has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Iushkova has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

153. The Notice Letter Plaintiff Iushkova received from Berry Dunn specifically directed her to take the actions described above. Indeed, the Notice Letter advised Plaintiff and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[31] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[32] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[33]

154. As a result of the Data Breach, Plaintiff Iushkova has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Iushkova fears that criminals will use her information to commit identity theft.

155. Plaintiff Iushkova anticipates spending considerable time and money on an ongoing basis.

156. Plaintiff Iushkova has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and continuing risk of injury flowing from fraud and identity theft posed by Plaintiff Iushkova's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Iushkova's Private Information that was entrusted to Defendants; (d) damages unjustly

[31] *See* Sample Notice Letter at n.19, *supra*.
[32] *Id.*
[33] *Id.*

retained by Defendants at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Iushkova's Private Information; and (e) continued risk to Plaintiff Iushkova's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Kathy Bishop's Experience

157. Plaintiff Kathy Bishop received a Notice Letter from Berry Dunn dated April 25, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

158. Plaintiff Kathy Bishop is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

159. Plaintiff Kathy Bishop stores any documents containing her Private Information in a safe and secure location. Plaintiff Kathy Bishop has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

160. Because of the Data Breach, Plaintiff Kathy Bishop's Private Information is now in the hands of cyber criminals.

161. Plaintiff Kathy Bishop has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

162. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number and PHI, Plaintiff Kathy Bishop is now subject to a present and continuing risk of crippling identity theft and fraud for her lifetime.

163. Since the Data Breach, Plaintiff Kathy Bishop has experienced identity theft in the form of unauthorized charges on her bank card, which caused Plaintiff Kathy Bishop to cancel and replace her card. Plaintiff Kathy Bishop has also experienced a substantial increase in spam and phishing calls, texts, and emails. For instance, Plaintiff Kathy Bishop has received fraudulent calls from callers claiming to be from the police, the Federal Bureau of Investigation ("FBI"), and/or Medicare/Medicaid. Plaintiff Kathy Bishop attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never experienced anything like this prior to now, and, to her knowledge, her Private Information has never been exposed in any other Data Breach.

164. As a result of the Data Breach, Plaintiff Kathy Bishop has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Kathy Bishop has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

165. The Notice Letter Plaintiff Kathy Bishop received from Berry Dunn specifically directed her to take the actions described above. Indeed, the Notice Letter advised Plaintiff and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[34] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit

[34] *See* Sample Notice Letter at n.19, *supra*.

reports."[35] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[36]

166. As a result of the Data Breach, Plaintiff Kathy Bishop has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Kathy Bishop fears that criminals will use her information to commit identity theft.

167. Plaintiff Kathy Bishop anticipates spending considerable time and money on an ongoing basis.

168. Plaintiff Kathy Bishop has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and continuing risk of injury flowing from fraud and identity theft posed by Plaintiff Kathy Bishop's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Kathy Bishop's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Kathy Bishop's Private Information; and (e) continued risk to Plaintiff Kathy Bishop's Private Information, which remains in the possession of Defendants and which is subject

[35] *Id.*
[36] *Id.*

to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Robert Hickman's Experience

169. Plaintiff Hickman received a Notice Letter from Berry Dunn dated April 25, 2024, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

170. Plaintiff Hickman is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

171. Plaintiff Hickman stores any documents containing his Private Information in a safe and secure location. Plaintiff Hickman has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

172. Because of the Data Breach, Plaintiff Hickman's Private Information is now in the hands of cyber criminals.

173. Plaintiff Hickman has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

174. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and PHI, Plaintiff Hickman is now subject to a present and continuing risk of crippling identity theft and fraud for his lifetime.

175. Since the Data Breach, Plaintiff Hickman has experienced identity theft in the form of receiving letters from debt collectors informing him that he owes a debt of approximately $1000 that he does not, in fact, owe. Plaintiff believes these letters to be fraudulent. Plaintiff Hickman has also experienced a substantial increase in spam and phishing phone calls, text messages, and emails. Plaintiff Hickman attributes the foregoing suspicious and unauthorized activity to the Data

Breach given the time proximity, the fact that he has never experienced anything like this prior to now, and, to his knowledge, his Private Information has never been exposed in any other Data Breach.

176. As a result of the Data Breach, Plaintiff Hickman has had no choice but to spend approximately 20 to 30 hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Hickman has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

177. The Notice Letter Plaintiff Hickman received from Berry Dunn specifically directed him to take the actions described above. Indeed, the Notice Letter advised Plaintiff and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[37] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[38] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[39]

[37] *See* Sample Notice Letter at n.19, *supra*.
[38] *Id.*
[39] *Id.*

178. As a result of the Data Breach, Plaintiff Hickman has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Hickman fears that criminals will use his information to commit identity theft.

179. Plaintiff Hickman anticipates spending considerable time and money on an ongoing basis.

180. Plaintiff Hickman has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and continuing risk of injury flowing from fraud and identity theft posed by Plaintiff Hickman's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Hickman's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Hickman's Private Information; and (e) continued risk to Plaintiff Hickman's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Sally Hughes's Experience

181. Plaintiff Hughes received a Notice Letter from Berry Dunn dated April 25, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

182. Plaintiff Hughes is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

183. Plaintiff Hughes stores any documents containing her Private Information in a safe and secure location. Plaintiff Hughes has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

184. Because of the Data Breach, Plaintiff Hughes's Private Information is now in the hands of cyber criminals.

185. Plaintiff Hughes has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

186. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number and PHI, Plaintiff Hughes is now subject to a present and continuing risk of crippling identity theft and fraud for her lifetime.

187. Since the Data Breach, Plaintiff Hughes has experienced identity theft in the form of various notices informing her that she has been approved for loans. Plaintiff Hughes has also experienced a substantial increase in spam and phishing phone calls. Plaintiff Hughes attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never experienced anything like this prior to now, and, to her knowledge, her Private Information has never been exposed in any other Data Breach.

188. As a result of the Data Breach, Plaintiff Hughes has had no choice but to spend 10 to 15 hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Hughes has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data

Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

189. The Notice Letter Plaintiff Hughes received from Berry Dunn specifically directed her to take the actions described above. Indeed, the Notice Letter advised Plaintiff and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[40] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[41] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[42]

190. As a result of the Data Breach, Plaintiff Hughes has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Hughes fears that criminals will use her information to commit identity theft.

191. Plaintiff Hughes anticipates spending considerable time and money on an ongoing basis.

192. Plaintiff Hughes has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and continuing risk of impending injury flowing from fraud and identity theft posed by Plaintiff Hughes's Private Information being placed in the hands of cybercriminals; (c) damages to and/or

[40] *See* Sample Notice Letter at n.19, *supra*.
[41] *Id.*
[42] *Id.*

diminution in value of Plaintiff Hughes's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff Hughes, including the difference in value between what Plaintiff Hughes should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Hughes's Private Information; and (e) continued risk to Plaintiff Hughes's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Donald Dee Smith's Experience

193. Plaintiff Smith received a Notice Letter from Berry Dunn dated April 25, 2024, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

194. Plaintiff Smith is very careful about sharing his sensitive information, and, to the best of his knowledge, has never had his Private Information exposed in another data breach.

195. Plaintiff Smith stores any documents containing his Private Information in a safe and secure location. Plaintiff Smith has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

196. Because of the Data Breach, Plaintiff Smith's Private Information is now in the hands of cyber criminals.

197. Plaintiff Smith has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

198. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and PHI, Plaintiff Smith is now subject to a present and continuing risk of crippling identity theft and fraud for his lifetime.

199. Since the Data Breach, Plaintiff Smith has experienced identity theft in the form of attempted Medicare fraud. An unknown person accessed Plaintiff Smith's personal email account. Plaintiff Smith also experienced an unauthorized withdrawal from his bank account for approximately $500. Plaintiff Smith also experienced at least one "hard" inquiry on his credit via TransUnion. Plaintiff Smith has also experienced a substantial increase in spam and phishing phone calls. Plaintiff Smith attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he has never experienced anything like this prior to now, and, to his knowledge, his Private Information has never been exposed in any other Data Breach.

200. As a result of the Data Breach, Plaintiff Smith has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Smith has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

201. The Notice Letter Plaintiff Smith received from Berry Dunn specifically directed him to take the actions described above. Indeed, the Notice Letter advised Plaintiff and all Class Members that they should "regularly review [their] credit reports and financial statements, and

immediately report any suspicious activity."[43] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[44] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[45]

202. As a result of the Data Breach, Plaintiff Smith has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Smith fears that criminals will use his information to commit identity theft.

203. Plaintiff Smith anticipates spending considerable time and money on an ongoing basis.

204. Plaintiff Smith has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Smith's valuable Private Information; (b) the present and continuing risk of injury flowing from fraud and identity theft posed by Plaintiff Smith's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Smith's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff Smith, including the difference in value between what Plaintiff Smith should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Smith's Private Information; and (e) continued risk to Plaintiff Smith's Private

[43] *See* Sample Notice Letter at n.19, *supra*.
[44] *Id.*
[45] *Id.*

Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Melody Bowman's Experience

205. Plaintiff Bowman received a Notice Letter from Berry Dunn dated April 25, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

206. Plaintiff Bowman is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

207. Plaintiff Bowman stores any documents containing her Private Information in a safe and secure location. Plaintiff Bowman has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

208. Because of the Data Breach, Plaintiff Bowman's Private Information is now in the hands of cyber criminals.

209. Plaintiff Bowman has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

210. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number and PHI, Plaintiff Bowman is now subject to a present and continuing risk of crippling identity theft and fraud for her lifetime.

211. Since the Data Breach, Plaintiff Bowman has experienced identity theft in the form of unauthorized charges requiring a replacement card as well as a substantial increase in spam and phishing calls, texts, and emails. Plaintiff Bowman attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she has never

experienced anything like this prior to now, and, to her knowledge, her Private Information has never been exposed in any other Data Breach.

212. As a result of the Data Breach, Plaintiff Bowman has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Bowman has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

213. The Notice Letter Plaintiff Bowman received from Berry Dunn specifically directed her to take the actions described above. Indeed, the Notice Letter advised Plaintiff Bowman and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[46] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[47] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[48]

214. As a result of the Data Breach, Plaintiff Bowman has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing

[46] *See* Sample Notice Letter at n.19, *supra*.
[47] *Id.*
[48] *Id.*

and misusing her Private Information. Plaintiff Bowman fears that criminals will use her information to commit identity theft.

215. Plaintiff Bowman anticipates spending considerable time and money on an ongoing basis.

216. Plaintiff Bowman has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and continuing risk of injury flowing from fraud and identity theft posed by Plaintiff Bowman's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Bowman's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Bowman's Private Information; and (e) continued risk to Plaintiff Bowman's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Brandy Brady's Experience

217. Plaintiff Brady received a Notice Letter from Berry Dunn dated April 25, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

218. Plaintiff Brady is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

219. Plaintiff Brady stores any documents containing her Private Information in a safe and secure location. Brady has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

220. Because of the Data Breach, Plaintiff Brady's Private Information is now in the hands of cyber criminals.

221. Plaintiff Brady has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

222. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number and PHI, Plaintiff Brady is now subject to a present and continuing risk of crippling identity theft and fraud for her lifetime.

223. Since the Data Breach, Plaintiff Brady has experienced a notable increase in spam and phishing phone calls and texts. Plaintiff Brady attributes the foregoing unauthorized activity to the Data Breach given the time proximity and, to her knowledge, her Private Information has never been exposed in any other Data Breach.

224. As a result of the Data Breach, Plaintiff Brady has expended her own money to purchase Lifelock identity protection services at a cost of approximately $90 per year. Plaintiff Brady enrolled in this service in April 2024 to help protect her Private Information following the Data Breach.

225. As a result of the Data Breach, Plaintiff Brady has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Brady has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data

Breach, researching and enrolling in identity protection services, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

226. The Notice Letter Plaintiff Brady received from Berry Dunn specifically directed her to take the actions described above. Indeed, the Notice Letter advised Plaintiff Brady and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[49] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[50] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[51]

227. As a result of the Data Breach, Plaintiff Brady has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Brady fears that criminals will use her information to commit fraud, which could cause monetary losses or damage to her credit.

228. Plaintiff Brady anticipates spending considerable time and money on an ongoing basis to deal with the ongoing impacts of the Data Breach.

229. Plaintiff Brady has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Brady's valuable Private Information; (b) the present and

[49] *See* Sample Notice Letter at n.19, *supra*.
[50] *Id.*
[51] *Id.*

continuing risk of impending injury flowing from fraud and identity theft posed by Plaintiff Brady's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Brady's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff Brady, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Brady's Private Information; and (e) continued risk to Plaintiff Brady's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Virginia Demel-Duff's Experience

230. Plaintiff Demel-Duff received a Notice Letter from Berry Dunn dated April 25, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

231. Plaintiff Demel-Duff is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

232. Plaintiff Demel-Duff stores any documents containing her Private Information in a safe and secure location. Plaintiff Demel-Duff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

233. Because of the Data Breach, Plaintiff Demel-Duff's Private Information is now in the hands of cyber criminals.

234. Plaintiff Demel-Duff has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

235. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number and PHI, Plaintiff Demel-Duff is now subject to a present and continuing risk of crippling identity theft and fraud for her lifetime.

236. As a result of the Data Breach, Plaintiff Demel-Duff has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Demel-Duff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

237. The Notice Letter Plaintiff Demel-Duff received from Berry Dunn specifically directed her to take the actions described above. Indeed, the Notice Letter advised Plaintiff Demel-Duff and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[52] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[53] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[54]

[52] *See* Sample Notice Letter at n.19, *supra*.
[53] *Id.*
[54] *Id.*

238. As a result of the Data Breach, Plaintiff Demel-Duff has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Demel-Duff fears that criminals will use her information to commit identity theft.

239. Plaintiff Demel-Duff anticipates spending considerable time and money on an ongoing basis to deal with the ongoing impacts of the Data Breach.

240. Plaintiff Demel-Duff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Demel-Duff's valuable Private Information; (b) the present and continuing risk of impending injury flowing from fraud and identity theft posed by Plaintiff Demel-Duff's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Demel-Duff's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff Demel-Duff, including the difference in value between what Plaintiff Demel-Duff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Demel-Duff's Private Information; and (e) continued risk to Plaintiff Demel-Duff's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Myron Nottingham's Experience

241. Plaintiff Nottingham received a Notice Letter from Berry Dunn dated April 25, 2024, informing him that his Private Information—including his PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

242. Plaintiff Nottingham is very careful about sharing his sensitive information.

243. Plaintiff Nottingham stores any documents containing his Private Information in a safe and secure location. Plaintiff Nottingham has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

244. Because of the Data Breach, Plaintiff Nottingham's Private Information is now in the hands of cyber criminals.

245. Plaintiff Nottingham has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

246. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number and PHI, Plaintiff Nottingham is now subject to a present and continuing risk of crippling identity theft and fraud for his lifetime.

247. Since the Data Breach, Plaintiff Nottingham has experienced identity theft in the form of unauthorized charges on his debit card in November/December 2023. In addition, Plaintiff Nottingham's recent background report reflected incorrect information attributed to him. Plaintiff Nottingham attributes the foregoing unauthorized and suspicious activity to the Data Breach given the time proximity, and the fact that he has never experienced anything like this prior to now.

248. In May 2024, as a result of the Data Breach, Plaintiff Nottingham purchased identity protection services for a cost of approximately $29.95.

249. As a result of the Data Breach, Plaintiff Nottingham has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Nottingham has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts

about the Data Breach, thoroughly reviewing account statements and other information, obtaining and reviewing copies of his credit reports, researching and enrolling in identity protection services, and taking other protective and ameliorative steps in response to the Data Breach.

250. The Notice Letter Plaintiff Nottingham received from Berry Dunn specifically directed him to take the actions described above. Indeed, the Notice Letter advised Plaintiff Nottingham and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[55] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[56] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[57]

251. As a result of the Data Breach, Plaintiff Nottingham has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Nottingham fears that criminals will use his information to commit identity theft.

252. Plaintiff Nottingham anticipates spending considerable time and money on an ongoing basis.

253. Plaintiff Nottingham has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and

[55] *See* Sample Notice Letter at n.19, *supra*.
[56] *Id.*
[57] *Id.*

continuing risk of injury flowing from fraud and identity theft posed by Plaintiff Nottingham's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Nottingham's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff Nottingham, including the difference in value between what Plaintiff Nottingham should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Nottingham's Private Information; and (e) continued risk to Plaintiff Nottingham's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Yasmine Encarnacion's Experience

254. Plaintiff Encarnacion received a Notice Letter from Berry Dunn dated April 25, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

255. Plaintiff Encarnacion is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

256. Plaintiff Encarnacion stores any documents containing her Private Information in a safe and secure location. Plaintiff Encarnacion has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

257. Because of the Data Breach, Plaintiff Encarnacion's Private Information is now in the hands of cyber criminals.

258. Plaintiff Encarnacion has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

259. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number and PHI, Plaintiff Encarnacion is now subject to a present and continuing risk of crippling identity theft and fraud for her lifetime.

260. As a result of the Data Breach, Plaintiff Encarnacion has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Encarnacion has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, placing freezes on her credit reports, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

261. The Notice Letter Plaintiff Encarnacion received from Berry Dunn specifically directed her to take the actions described above. Indeed, the Notice Letter advised Plaintiff Encarnacion and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[58] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[59] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[60]

[58] *See* Sample Notice Letter at n.19, *supra*.
[59] *Id.*
[60] *Id.*

262. As a result of the Data Breach, Plaintiff Encarnacion has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Encarnacion fears that criminals will use her information to commit identity theft.

263. Plaintiff Encarnacion anticipates spending considerable time and money on an ongoing basis to deal with the ongoing impacts of the Data Breach.

264. Plaintiff Encarnacion has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Encarnacion's valuable Private Information; (b) the present and continuing risk of impending injury flowing from fraud and identity theft posed by Plaintiff Encarnacion's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Encarnacion's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff Encarnacion, including the difference in value between what Plaintiff Encarnacion should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Encarnacion's Private Information; and (e) continued risk to Plaintiff Encarnacion's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

Plaintiff Tonya Gambino's Experience

265. Plaintiff Gambino received a Notice Letter from Berry Dunn dated April 25, 2024, informing her that her Private Information—including her PII and PHI—was specifically identified as having been exposed to cybercriminals in the Data Breach.

266. Plaintiff Gambino is very careful about sharing her sensitive information, and, to the best of her knowledge, has never had her Private Information exposed in another data breach.

267. Plaintiff Gambino stores any documents containing her Private Information in a safe and secure location. Gambino has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

268. Because of the Data Breach, Plaintiff Gambino's Private Information is now in the hands of cyber criminals.

269. Plaintiff Gambino has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

270. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number and PHI, Plaintiff Gambino is now subject to a present and continuing risk of crippling identity theft and fraud for her lifetime.

271. Since the Data Breach, Plaintiff Gambino has experienced a notable increase in spam and phishing emails and texts. Plaintiff Gambino attributes the foregoing suspicious activity to the Data Breach given the time proximity and, that she had not previously experienced this degree and type of spam and phishing correspondence.

272. As a result of the Data Breach, Plaintiff Gambino has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Data Breach. Among other things, Plaintiff Gambino has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate and mitigate the future consequences of the Data Breach, including researching facts about the Data Breach, researching and enrolling in identity protection services, thoroughly

reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach.

273. The Notice Letter Plaintiff Gambino received from Berry Dunn specifically directed her to take the actions described above. Indeed, the Notice Letter advised Plaintiff Gambino and all Class Members that they should "regularly review [their] credit reports and financial statements, and immediately report any suspicious activity."[61] The Notice Letter further stated: "We recommend that you remain vigilant by reviewing account statements and monitoring credit reports."[62] In addition, the Notice Letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, placing fraud alerts with credit reporting bureaus, placing security freezes on credit reports, filing a complaint with the FTC, and obtaining information about identity theft and fraud.[63]

274. As a result of the Data Breach, Plaintiff Gambino has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Gambino fears that criminals will use her information to commit identity theft.

275. Plaintiff Gambino anticipates spending considerable time and money on an ongoing basis to deal with the ongoing impacts of the Data Breach.

276. Plaintiff Gambino has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the present and continuing risk of impending injury flowing from fraud and identity theft posed by Plaintiff

[61] *See* Sample Notice Letter at n.19, *supra*.
[62] *Id.*
[63] *Id.*

Gambino's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Gambino's Private Information that was entrusted to Defendants; (d) damages unjustly retained by Defendants at the cost to Plaintiff Gambino, including the difference in value between what Plaintiff Gambino should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Gambino's Private Information; and (e) continued risk to Plaintiff Gambino's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

277. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

278. Plaintiffs and Class Members entrusted their Private Information to Defendants in order to receive Defendants' services.

279. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices.

280. As a direct and proximate result of Defendants' actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns and insurance claims filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

281. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

282. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

283. Plaintiffs and Class Members entrusted their inherently valuable Private Information to Defendants with the understanding that it would be accompanied by adequate data security. It was not. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

284. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[64] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[65]

285. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and

[64] *See How Data Brokers Profit From the Data We Create*, the Quantum Record (Apr. 5, 2023), https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion.

[65] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Apr. 29, 2024).

diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

286. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

287. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendants, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its clients' patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

288. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

289. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

290. Specifically, Plaintiffs propose the following Nationwide Class (referred to herein as the "Class"), subject to amendment as appropriate:

> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a Notice Letter.

291. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

292. Plaintiffs reserve the right to modify or amend the definition of the proposed Nationwide Class, as well as add subclasses, before the Court determines whether certification is appropriate.

293. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

294. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of over two million impacted individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendants' records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the FTCA;

c. When Defendants learned of the Data Breach;

d. Whether Defendants' response to the Data Breach was adequate;

e. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

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

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

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

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

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

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

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

o. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants' conduct was *per se* negligent;

r. Whether Defendants were unjustly enriched;

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

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

296. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

297. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

298. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common

issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

300. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

301. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
AS TO DEFENDANT BERRY DUNN
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

302. Plaintiffs restate and reallege paragraphs 1 through 301 as if fully set forth herein.

303. Berry Dunn knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

304. Berry Dunn's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

305. Berry Dunn knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Berry Dunn was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

306. Berry Dunn owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Berry Dunn's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect its clients' patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

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

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

307. Berry Dunn's duty to employ reasonable data security measures arose, in part, under Section 5 of the FTCA, 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.

308. Berry Dunn's' duty also arose because Berry Dunn was bound by industry standards to protect its clients' patients' confidential Private Information.

309. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Berry Dunn, and Berry Dunn owed them a duty of care to not subject them to an unreasonable risk of harm.

310. Berry Dunn, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Berry Dunn's possession.

311. Berry Dunn, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

312. Berry Dunn, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

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

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

b. Failing to adequately monitor the security of its networks and systems and those of its third-party vendors, including Reliable Networks;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

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

e. Failing to comply with the FTCA;

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

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

314. Berry Dunn acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

315. Berry Dunn had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Berry Dunn with their Private Information was predicated on the understanding that Berry Dunn would take adequate security precautions. Moreover, only Berry Dunn had the ability to protect its systems (and the Private Information that it stored on them) from attack.

316. Berry Dunn's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

317. As a result of Berry Dunn's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

318. Berry Dunn's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

319. As a result of Berry Dunn' negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

320. Berry Dunn also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

321. As a direct and proximate result of Berry Dunn's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

322. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

323. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

324. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Berry Dunn to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE
AS TO DEFENDANT RELIABLE NETWORKS
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

325. Plaintiffs restate and reallege paragraphs 1 through 301 as if fully set forth herein.

326. Reliable Networks knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

327. Reliable Networks' duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

328. Reliable Networks knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Reliable Networks was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

329. Reliable Networks owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Reliable Networks' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect its clients' patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

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

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

330. Reliable Networks' duty to employ reasonable data security measures arose, in part, under Section 5 of the FTCA, 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.

331. Reliable Networks' duty also arose because Reliable Networks was bound by industry standards to protect the confidential Private Information in its possession.

332. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Reliable Networks, and Reliable Networks owed them a duty of care to not subject them to an unreasonable risk of harm.

333. Reliable Networks, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within its possession.

334. Reliable Networks, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

335. Reliable Networks, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

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

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

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

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

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

e. Failing to comply with the FTCA;

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

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

337. Reliable Networks acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

338. Reliable Networks had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Reliable Networks with their Private Information was predicated on the understanding that Reliable Networks would take adequate security precautions. Moreover, only Reliable Networks had the ability to protect its systems (and the Private Information that it stored on them) from attack.

339. Reliable Networks' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

340. As a result of Reliable Networks' ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

341. Reliable Networks' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

342. As a result of Reliable Networks' negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

343. Reliable Networks also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

344. As a direct and proximate result of Reliable Networks' negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

345. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

346. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

347. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Reliable Networks to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
NEGLIGENCE *PER SE*
AS TO DEFENDANT BERRY DUNN
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

348. Plaintiffs restate and reallege paragraphs 1 through 301 as if fully set forth herein.

349. Pursuant to Section 5 of the FTCA, Berry Dunn had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

350. Berry Dunn breached its duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

351. Specifically, Berry Dunn breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

352. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Berry Dunn's duty in this regard.

353. Berry Dunn also violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

354. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Berry Dunn's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

355. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect and Berry Dunn's failure to comply with both constitutes negligence *per se*.

356. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Berry Dunn's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

357. As a direct and proximate result of Berry Dunn's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

358. As a direct and proximate result of Berry Dunn's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

359. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Berry Dunn to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV
NEGLIGENCE *PER SE*
AS TO DEFENDANT RELIABLE NETWORKS
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

360. Plaintiffs restate and reallege paragraphs 1 through 301 as if fully set forth herein.

361. Pursuant to Section 5 of the FTCA, Reliable Networks had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

362. Reliable Networks breached its duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

363. Specifically, Reliable Networks breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

364. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Reliable Networks' duty in this regard.

365. Reliable Networks also violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

366. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Reliable Networks' networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

367. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect and Reliable Networks' failure to comply with both constitutes negligence *per se*.

368. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Reliable Networks' negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

369. As a direct and proximate result of Reliable Networks' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

370. As a direct and proximate result of Reliable Networks' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

371. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Reliable Networks to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

372. Plaintiffs restate and reallege paragraphs 1 through 301 as if fully set forth herein.

373. Plaintiffs and Class Members conferred a benefit on Defendants by turning over their Private Information to Defendants and by paying for products and services, directly or indirectly, that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

374. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including from payments made to it, directly or indirectly, by Plaintiffs and Class Members.

375. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

376. Defendants have retained the benefits of their unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that they failed to provide.

377. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them, which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments they received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

378. If Plaintiffs and Class Members had known that Defendants had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendants.

379. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

380. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) the loss of the opportunity to control how their Private

Information is used; (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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in its continued possession; (vi) the actual misuse of the compromised Private Information and the time and costs associated therewith; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

381. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

382. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
AS TO DEFENDANT BERRY DUNN
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

383. Plaintiffs restate and reallege paragraphs 1 through 301 as if fully set forth herein.

384. Berry Dunn entered into contracts, written or implied, with its clients to perform services that include, but are not limited to, providing consulting and accounting services. Upon information and belief, these contracts are virtually identical between and among Berry Dunn and its clients around the country whose patients, including Plaintiffs and Class Members, were affected by the Data Breach.

385. In exchange, Berry Dunn agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiffs and the Class.

386. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Berry Dunn and its clients. Berry Dunn knew that if it were to breach these contracts with its clients, the clients' patients—Plaintiffs and Class Members—would be harmed.

387. Berry Dunn breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiffs and Class Members thereof.

388. Plaintiffs and the Class were harmed by Berry Dunn's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

389. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT VII
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
AS TO DEFENDANT RELIABLE NETWORKS
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

390. Plaintiffs restate and reallege paragraphs 1 through 301 as if fully set forth herein.

391. Reliable Networks entered into a contract, written or implied, with Berry Dunn to perform services that include, but are not limited to, cloud hosting, managed services, IT consulting and security.

392. In exchange, Reliable Networks agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiffs and the Class.

393. This contract was made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contract entered into between Reliable Networks and Berry Dunn. Reliable Networks knew that if it were to breach this contract with Berry Dunn, Berry Dunn's clients' patients—Plaintiffs and Class Members—would be harmed.

394. Reliable Networks breached the contract it entered into with Berry Dunn by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiffs and Class Members thereof.

395. Plaintiffs and the Class were harmed by Reliable Network's breach of its contract with Berry Dunn, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

396. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT VIII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

397. Plaintiffs restate and reallege paragraphs 1 through 301 as if fully set forth herein.

398. 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 to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

399. Defendants owe a duty of care to Plaintiffs and Class Members, which required them to adequately secure Plaintiffs' and Class Members' Private Information.

400. Defendants still possess the Private Information of Plaintiffs and Class Members.

401. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

402. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure their clients, and their clients' patients' Private Information and to timely notify individuals of a data breach under the common law and the FTCA;

b. Defendants' existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect their clients, and their clients' patients' Private Information; and

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure individuals' Private Information.

403. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect individuals' Private Information, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

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

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

v. conducting regular database scanning and security checks;

vi. 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; and

vii. meaningfully educating Defendants' clients and their patients about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

404. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach of Defendants systems. The risk of another such breach is real, immediate, and substantial. If another breach at Berry Dunn or Reliable Networks occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

405. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

406. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Berry Dunn or Reliable Networks, thus preventing future injury to Plaintiffs and other patients whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Quinton Anderson, Michael Meyerson, Laura Russell, Kathy Bishop, Randy Bishop, Kristie Iushkova, Robert Hickman, Sally Hughes, Donald Dee Smith, Melody Bowman, Brandy Brady, Virginia Demel-Duff, Myron Nottingham, Yasmine Encarnacion, and Tonya Gambino, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: June 18, 2024.

Respectfully submitted,

By: */s/ David E. Bauer*
David E. Bauer, Bar No 3609
443 Saint John Street
Portland, Maine 04102
Tel: (207) 804-6296
david.edward.bauer@gmail.com

Mason A. Barney (admitted *pro hac vice*)
Tyler J. Bean (admitted *pro hac vice*)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Bryan L. Bleichner (admitted *pro hac vice*)
Philip J. Krzeski (admitted *pro hac vice*)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Tel: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Jeff Ostrow (admitted *pro hac vice*)
KOPELOWITZ OSTROW P.A.
One West Las Olas Boulevard, Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

Interim Co-Lead Counsel

Mariya Weekes (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: (786) 879-8200
Fax: (786) 879-7520
mweekes@milberg.com

Joseph M. Lyon (admitted *pro hac vice*)
Kevin M. Cox (admitted
THE LYON FIRM
2754 Erie Avenue
Cincinnati Ohio 45208
Tel: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com
kcox@thelyonfirm.com

Daniel Srourian, Esq. (admitted *pro hac vice*)
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Tel: (213) 474-3800
Fax: (213) 471-4160
daniel@slfla.com

A. Brooke Murphy (admitted *pro hac vice*)
MURPHY LAW FIRM
4116 Wills Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Tel: (405) 389-4989
abm@murphylegalfirm.com

Charles E. Schaffer (admitted *pro hac vice*)
LEVIN SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com

Brett R. Cohen (admitted *pro hac vice*)
LEEDS BROWN LAW, P.C.
One Old Country Road, Suite 347
Carle Place, NY 11514-1851
Tel: (516) 873-9550
bcohen@leedsbrownlaw.com

Jeffrey Goldenberg (*pro hac vice* forthcoming)

GOLDENBERG SCHNEIDER, L.P.A.
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Tel: (513) 345-8297
Email: jgoldenberg@gs-legal.com

Carl Malmstrom (admitted *pro hac vice*)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 West Jackson, Ste. 1700
Chicago, IL 60604
Tel: (312) 984-0000
malmstrom@whafh.com

Alexander E. Spadinger (*pro hac vice* forthcoming)
SHAHEEN & GORDON
353 Central Ave.
2nd Floor
Dover, New Hampshire 03301
Tel: (603) 749-5000
Fax: (603) 749-1838
aspadinger@shaheengordon.com

James J. Pizzirusso (*pro hac vice* forthcoming)
HAUSFELD LLP
888 16th St., N.W.
Suite 300
Washington, D.C. 20006
Tel: (202) 540-7200
jpizzirusso@hausfeld.com

Matthew Fornaro (*pro hac vice* forthcoming)
MATHEW FORNARO PA
11555 Heron Bay Blvd., Ste. 200
Coral Springs, Florida FL 33076
Tel: (954) 324-3651
Fax: (954) 248-2099
mfornaro@fornarolegal.com

Marc H. Edelson
EDELSON LECHTZIN LLP
411 S. State Street
Suite N300
Newtown, PA 18940
Tel: (215) 867-2399
medelson@edelson-law.com

Attorneys for Plaintiffs and Putative Class