IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA
WHEELING DIVISION

Charles Milliken Jr and Mary Kay Milliken, *On behalf of themselves and all others similarly situated,* Plaintiffs, v. Bayer Heritage Federal Credit Union., Defendant.	Case No. 5:24-cv-57 Bailey 3/20/2024 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Charles Milliken Jr. and Mary Kay Milliken ("Plaintiffs") brings this Class Action Complaint, on behalf of themselves and all others similarly situated (the "Class Members"), against Defendant Bayer Heritage Federal Credit Union. ("Defendant") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data security breach ("Data Breach") on Defendant's network that resulted in unauthorized access to highly sensitive patient personal information and medical data. As a result of the Data Breach, Plaintiff and thousands of Class Members, including approximately 61,000 individuals, suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy

or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive personal information.

2. In addition, Plaintiffs and Class Members' sensitive personal information—which was entrusted to Defendant, its officials, and its agents—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes names Social Security numbers, date of birth, driver's license numbers and/or state identification numbers, passports, direct deposit bank information, ("Personally Identifying Information", "Personal Information" or "PII"). The PII that Defendant collected and maintained will be collectively referred to as the "Private Information."

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiffs' and Class Members' Private Information that Defendant collected and maintained, and for Defendant's failure to (1) provide timely and adequate notice to Plaintiff and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party, and (2) identify precisely what specific type of information was accessed.

5. Defendant maintained the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant

was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a vulnerable condition.

6. In addition, upon information and belief, Defendant failed to properly monitor the computer network and IT systems that housed the Private Information.

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

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including 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' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns 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.

9. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts and credit to guard against identity theft.

10. Plaintiffs and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. By his Complaint, Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

12. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

13. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract; and (iii) unjust enrichment.

THE PARTIES

A. Plaintiff Charles Miliken Jr.

14. Plaintiff Charles Miliken Jr. is a natural person, resident, and a citizen of the State of West Virginia and resides in Wetzel County. Plaintiff has no intention of moving to a different state in the immediate future. Plaintiff is acting on his own behalf and on behalf of others similarly situated. Upon information and belief Defendant obtained and continues to maintain Plaintiff's Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff would not have entrusted his Private Information to Defendant had he known that Defendant failed to maintain adequate data security practices or safeguards. Plaintiff's Private Information was compromised and disclosed as a result of Defendant's inadequate data security practices, which resulted in the Data Breach.

B. Plaintiff Mary Kay Milliken

15. Plaintiff Charles Miliken Jr. is a natural person, resident, and a citizen of the State of West Virginia and resides in Wetzel County. Plaintiff has no intention of moving to a different state in the immediate future. Plaintiff is acting on his own behalf and on behalf of others similarly situated. Upon information and belief Defendant obtained and continues to maintain Plaintiff's Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff would not have entrusted his Private Information to Defendant had he known that Defendant failed to maintain adequate data security practices or safeguards. Plaintiff's Private Information was compromised and disclosed as a result of Defendant's inadequate data security practices, which resulted in the Data Breach.

16. **Defendant Bayer Heritage Federal Credit Union.**

17. Defendant Bayer Heritage Federal Credit Union is corporation with its principal place of business located at 788 N. State Route 2 New Martinsville, West Virginia 26155.

JURISDICTION AND VENUE

18. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, are citizens of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

19. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal place of business is in this District, and it regularly conducts business in West Virginia, and has sufficient minimum contacts in West Virginia.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. DEFENDANT'S BUSINESS

21. Defendant is a credit union in West Virginia and the surrounding areas.

22. In order to obtain banking services from Defendant, Defendant requires its patients to provide sensitive and confidential Private Information, including their names, Social Security numbers, date of birth, driver's license numbers and/or state identification numbers, passports, direct deposit bank information, medical information, health insurance information, and likely other sensitive information.

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

24. Upon information and belief, Defendant made promises and representations to its patients that the Private Information collected from them as a condition of obtaining medical services at Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

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

26. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

27. On information and belief, in the ordinary course of its business, Defendant maintains the Private Information of customers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Photo identification;
- Employment information, and;
- Other information that Defendant may deem necessary to provide care.

28. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to customers, Defendant, upon information and

belief, promises to, among other things: comply with industry standards related to data security and Private Information; inform employees of its legal duties and comply with all federal and state laws protecting current and former patient Private Information; only use and release Private Information for reasons that relate to Defendant's business; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

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

30. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

31. Plaintiffs and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business purposes, and to prevent the unauthorized disclosures of the Private Information.

B. THE CYBERATTACK

32. On or about October 31, 2023, Defendant became aware that an unauthorized party gained access to Defendant's computer systems.

33. Defendant took steps to secure its systems and investigate the nature and scope of the incident on the network.

34. Through its investigation, Defendant determined that its network and servers were subject to a cyber-attack that impacted its network where information on its network was accessed and acquired without authorization.

35. The investigation determined that files on Defendant's network were accessed by an unauthorized user from October 31, 2023, through November 1, 2023.

36. Upon information and belief, Plaintiffs' and Class Members' Private Information was encrypted, exfiltrated, and stolen in the attack.

37. Furthermore, the investigation determined that the accessed systems contained Private Information, which was accessible, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

38. The type of Private Information accessed by the unauthorized actor in the Data Breach includes names, Social Security numbers, date of birth, driver's license numbers and/or state identification numbers, passports, direct deposit bank information, and likely other sensitive information.

39. As a result of the Data Breach, Defendant took steps to secure the network, and launched an investigation to determine the nature and scope of the incident. In addition, the investigation revealed that approximately 61,000 individuals, and likely many more, were victims of the Data Breach.

40. While Defendant stated in the notice letter that the unusual activity occurred and was discovered in October 2023, Defendant did not begin notifying victims until late January 2024 – nearly three months after they discovered the Data Breach.

41. Upon information and belief, and based on the type of cyberattack, along with public news reports, it is plausible and likely that Plaintiff's Private Information was stolen in the Data Breach. Plaintiff further believes his Private Information was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals.

42. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

44. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the industry preceding the date of the breach.

45. In light of recent high profile data breaches at other companies, Defendant knew or should have known that their electronic records and patient Private Information would be targeted by cybercriminals and ransomware attack groups.

46. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

C. DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

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

48. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[1] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[2]

49. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

[1] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 7, 2024).
[2] *Id*.

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

51. These FTC enforcement actions include actions against companies like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

52. Defendant failed to properly implement basic data security practices.

53. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

54. Defendant was at all times fully aware of its obligation to protect the Private Information of patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

55. As shown above, experts studying cybersecurity routinely identify companies in the medical industry as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

56. Several best practices have been identified that at a minimum should be implemented by Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

57. Other best cybersecurity practices that are standard in the medical industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

58. Defendant 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.

59. These foregoing frameworks are existing and applicable industry standards in the medical industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

E. DEFENDANT'S BREACH

60. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect Private Information;

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

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

g. Failing to adhere to industry standards for cybersecurity as discussed above; and

h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

61. During January 2024, Defendant, began sending Plaintiff and other Data Breach victims, informing them that:

> We recently learned that an unauthorized party gained access to certain Bayer Heritage computer systems. Upon discovering the incident, we promptly took steps to contain it. We also engaged a leading, third-party forensic investigation firm to confirm the security of our systems and to further investigate. Based on the results of the investigation, we believe that the unauthorized party acquired copies of certain Bayer Heritage files between October 31, 2023 and November 1, 2023..[3]

62. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

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

64. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs

[3]https://apps.web.maine.gov/online/aeviewer/ME/40/dfbd4fa8-a7ba-482c-be99-5700946e008f.shtml (last visited Feb. 7, 2014).

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

65. The attacker accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members, including their private medical information and other sensitive information. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

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

67. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

F. CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT INDIVIDUALS AT AN INCREASED RISK OF FRAUD AND IDENTITY THEFT

68. Cyberattacks and data breaches at companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

69. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[4]

[4] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Feb. 7, 2024).

70. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable 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, take over victims' identities in order to engage in illegal financial transactions under the victims' names. 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 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 information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

71. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[5]

[5] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Feb. 7, 2024).

72. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

73. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[6]

74. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

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

76. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

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

77. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

78. There is a strong probability that entire batches of stolen information are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

79. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

80. Private Information can sell for as much as $363 per record according to the Infosec Institute.[7] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

81. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[8]

[7] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market (last visited Feb. 7, 2024).

[8] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 7, 2024).

82. For this reason, Defendant knew or should have known about these dangers and strengthened its data and systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

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

84. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[9]

85. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

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

[9] How to Protect Your Networks from RANSOMWARE, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Feb. 7, 2024).

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

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

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

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

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

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

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

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

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

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

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[10]

86. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

[10] *Id*. at 3-4.

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[11]

87. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

88. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of more than 61,000 current and former patients, including Plaintiff and Class Members.

G. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

89. To date, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

90. Defendant has merely instructed Plaintiffs and Class Members to "remain vigilant", but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

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

92. Plaintiffs' and Class Members' personal information, including but not limited to, names, Social Security numbers, date of birth, driver's license numbers and/or

[11] See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Feb. 7, 2024).

state identification numbers, passports, direct deposit bank information, and likely other sensitive information, were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

93. Since being notified of the Data Breach, Plaintiffs have spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

94. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, considering cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

95. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

96. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

97. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

98. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

99. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as

potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members. Plaintiffs have already experienced various phishing attempts by telephone and through electronic mail.

100. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

101. Plaintiffs and Class Members also suffered a loss of value of their Private Information 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.

102. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer system and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for and agreed to.

103. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their accounts and sensitive information for misuse.

104. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

105. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

106. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

107. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

H. PLAINTIFF CHARLES MILIKEN JR.'S EXPERIENCE

108. Plaintiff Charles Milliken Jr. is a customer of Defendant.

109. As a condition of obtaining services from Defendant, Plaintiff Charles Milliken entrusted his Private Information to Defendant with the reasonable expectation and understanding that Defendant would take at a minimum industry standard precaution to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify his of any data security incidents related to his. Plaintiff Charles Milliken would not have used Defendant's services had he known that Defendant would not take reasonable steps to safeguard his Private Information.

110. In January 2024, months after Defendant learned of the data breach, Plaintiff Charles Milliken received a letter from Defendant, notifying him that his Private Information had been improperly accessed and/or obtained by unauthorized third parties.

111. As a result of the Data Breach, Plaintiff Charles Milliken made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach reviewing credit card and financial account statements. He also intends to order a copy of his credit report and reach out to his insurance company to review those records as well to ensure that he has not been subject to any fraud. He also has and is in the process of changing passwords. He is also researching credit monitoring services to find an affordable option.

112. Plaintiff Charles Milliken has spent multiple hours attempting to mitigate the effects of the breach and safeguard himself from its consequences. He will continue to spend time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

113. Plaintiff Charles Milliken suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Charles Milliken; (b) violation of his privacy rights; (c) the likely theft of his Private Information; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

114. Plaintiff Charles Milliken has also suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Charles Milliken is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff Charles Milliken also has suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to his medical records and prescriptions.

115. As a result of the Data Breach, Plaintiff Charles Milliken anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Charles Milliken will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

I. PLAINTIFF MARY KAY MILLIKEN.'S EXPERIENCE

116. Plaintiff Mary Kay Milliken is a customer of Defendant.

117. As a condition of obtaining services from Defendant, Plaintiff Mary Kay Milliken entrusted her Private Information to Defendant with the reasonable expectation and understanding that Defendant would take at a minimum industry standard precaution to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her Personal Information. Plaintiff Mary Kay Milliken would not have used Defendant's services had she known that Defendant would not take reasonable steps to safeguard her Private Information.

118. In January 2024, months after Defendant learned of the data breach, Plaintiff Mary Kay Milliken received a letter from Defendant, notifying her that her Private Information had been improperly accessed and/or obtained by unauthorized third parties.

119. As a result of the Data Breach, Plaintiff Mary Kay Milliken made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach reviewing credit card and financial account statements. She also intends to order a copy of her credit report and reach out to her insurance company to review those records as well to ensure that she has not been subject to any fraud. She also has and is in the process of changing passwords. She is also researching credit monitoring services to find an affordable option.

120. Plaintiff Mary Kay Milliken has spent multiple hours attempting to mitigate the effects of the breach and safeguard herself from its consequences. She will continue to

spend time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

121. Plaintiff Mary Kay Milliken suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Mary Kay Milliken; (b) violation of her privacy rights; (c) the likely theft of her Private Information; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

122. Plaintiff Mary Kay Milliken has also suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Mary Kay Milliken is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff Mary Kay Milliken also has suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to his medical records and prescriptions.

123. As a result of the Data Breach, Plaintiff Mary Kay Milliken anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Mary Kay Milliken will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

CLASS ACTION ALLEGATIONS

124. Plaintiffs brings this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

125. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **All persons in the United States whose Private Information was maintained on Defendant's computer systems and network that were compromised in the Data Breach announced by Defendant Bayer Heritage Federal Credit Union in January 2024 (the "Class").**

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

127. Plaintiffs reserve the right to amend or modify the Class definition as this case progresses.

128. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately 61,000 individuals whose sensitive data was compromised in Data Breach at Bayer Heritage Federal

129. **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 Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

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

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

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

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

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

130. **Typicality**. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

131. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

132. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's 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.

133. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. 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 Defendant. In contrast, the conduct of 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.

134. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

135. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

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

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

CAUSES OF ACTION

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

137. Plaintiffs re-allege and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

138. Defendant required individuals, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of its business.

139. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the

information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

141. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and patients, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

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

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

144. Defendant 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 Defendant include, but are not limited to, the following:

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

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

c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

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

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.

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

146. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

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

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

149. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' Private Information.

150. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

151. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

152. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

153. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

154. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

SECOND COUNT
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

155. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth herein.

156. Plaintiffs and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

157. Plaintiffs and the Class were required to and delivered their Private Information to Defendant as a condition of obtaining medical products and services from Defendant.

158. Defendant DMOS solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

159. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing banking services to Plaintiffs and Class Members.

160. In accepting such information and payment for services, Plaintiffs and the other Class Members entered into an implied contract with Defendant whereby Defendant

became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

161. In delivering their Private Information to Defendant, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard the data as part of their employment.

162. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

163. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

164. Plaintiffs and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

165. Had Defendant disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Sensitive Information to Defendant.

166. Defendant recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

167. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with Defendant.

168. Defendant breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

169. As a direct and proximate result of Defendant's conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

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

170. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

171. This count is pleaded in the alternative to Count 2 (breach of implied contract).

172. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including funds made as a result of the business from Plaintiffs and the Class Members.

173. As such, a portion of the revenue made as a result of the business of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the

amount of the portion of each payment made that is allocated to data security is known to Defendant.

174. Plaintiffs and Class Members conferred a monetary benefit on Defendant. In exchange, Plaintiffs and Class Members should have received adequate data security protecting their Private Information.

175. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

176. Plaintiffs and Class Members conferred a benefit on Defendant, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' Personal Information, and by providing Defendant with their valuable Personal Information.

177. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

178. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money that should have been used on data security, because

Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

179. Defendant acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

180. If Plaintiffs and Class Members knew that Defendant had not secured their Personal Information, they would not have agreed to provide their Personal Information to Defendant.

181. Plaintiffs and Class Members have no adequate remedy at law.

182. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personal Information; (v) 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; (vi) the continued risk to their Personal Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Personal Information in their continued possession; 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 Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

183. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

184. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representative and their counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

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

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Under Federal of Civil Procedure 38(b), Plaintiff demands a trial by jury on any and all issues in this action so triable.

Respectfully Submitted,

Dated: March 20, 2024

By:*/s/ Lee A. Floyd*

Lee A. Floyd (WVB # 11823)
BREIT BINIAZAN, PC
2100 E. Cary Street, Suite 310
Richmond, Virginia 23223
(804) 351-9040
(757) 670-3939
Lee@bbtrial.com

Gary M. Klinger *(Pro Hac Vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606

Phone: 866.252.0878
Email: gklinger@milberg.com

Philip J. Krzeski (*Pro Hac Vice* forthcoming)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
pkrzeski@chestnutcambronne.com

Counsel for Plaintiff and the Class

ClassAction.org
