IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING

MICHAEL BERGESON, individually and on behalf of all others similarly situated, Plaintiff, v. VIRGINIA MASON MEDICAL CENTER, Defendant.	Case No. **CLASS ACTION COMPLAINT**

CLASS ACTION COMPLAINT

Plaintiff Michael Bergeson, individually, and on behalf of all others similarly situated, brings this action against Defendant Virginia Mason Medical Center ("VMMC" or "Defendant"), a Washington corporation, to obtain damages, restitution and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. VMMC is a health-care provider that provides medical services to patients in the city of Seattle and throughout the Seattle metropolitan area.

2. As a condition of providing health services to patients, VMMC requires patients to

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

provide sensitive and private information including but not limited to patient names, addresses, dates of birth, Social Security numbers, and driver's license numbers, health insurance plan information and IDs, financial information, and medical and clinical information.

3. Between the dates of December 21, 2021, and January 3, 2022, an unauthorized person or persons gained unauthorized access to VMMC's employee email accounts, purportedly through a successful phishing attempt, and obtained access to confidential files containing patients' and employees' Private Information (the "Data Breach").

4. For nearly two weeks, the cybercriminals who hacked into VMMC's network had access to files containing information pertaining to VMMC's patients including Plaintiff, as well as VMMC's employees.

5. Defendant only became aware of the hacking incident and Data Breach in January 2022. As a result of the Data Breach, Plaintiff and thousands of Class Members, suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their personal information.

6. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third parties, remains also in the possession of Defendant, and without additional safeguards and independent review and oversight, remains vulnerable to additional hackers and theft.

7. Information compromised in the Data Breach includes patient names, addresses,

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

dates of birth, Social Security numbers, email addresses, health insurance company and plan member IDs, as well as information related to COVID screening, vaccinations, and surveillance efforts, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") that Defendant collected and maintained (collectively the "Private Information").

8. VMMC did not notify patients that their Private Information was subject to unauthorized access resulting from the Data Breach until May 26, 2022, nearly six (6) months after the attack was launched and the Data Breach was discovered.

9. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' and employees' Private Information.

10. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

11. Defendant VMMC maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

12. The mechanism of the hacking and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant and entities like it, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

from those risks left that property in a dangerous condition and vulnerable to theft.

13. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt notice of the Data Breach.

14. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for nearly two full weeks.

15. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

16. Armed with the Private Information accessed in the Data Breach, 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 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.

17. As a result of the Data Breach, Plaintiff and Class Members have been exposed to

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

a present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

18. Plaintiff and Class Members will incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

19. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

20. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

21. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of himself and the putative Class.

PARTIES

22. Plaintiff Michael Bergeson is, and at all times mentioned herein was, an individual citizen of the State of Washington residing in the City of Snohomish. Plaintiff Bergeson was a patient at VMMC and received medical services and treatment from Defendant. At the time of receiving services, he was required to and did provide his Private Information to Defendant. Plaintiff was notified of Defendant's Data Breach and his Private Information being compromised upon receiving a notice letter dated May 26, 2022.

23. Defendant VMMC is a health-care services provider with its principal place of business at 1100 9th Ave., Seattle, Washington 98101.

JURISDICTION AND VENUE

24. This Court has jurisdiction over Defendant because Defendant is organized under

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

the laws of the State of Washington and the causes of action alleged herein arise from Defendant transacting business in Washington.

25. Venue is proper in this county pursuant to Wash. Rev. Code § 4.12.025 because Defendant maintains its principal offices and conducts significant business activities in this county, and maintains its registered office at 1100 9th Ave., Seattle, Washington 98101. In addition, venue is proper because a substantial part of the events and omissions giving rise to this action occurred in this county.

DEFENDANT'S BUSINESS

26. Defendant VMMC is a health-care services provider that offers medical services and treatments throughout the Seattle metropolitan area. VMMC is part of the larger Virginia Mason Franciscan Health, which is one of the largest healthcare providers in the greater Seattle area.

27. VMMC provides a wide range of medical and surgical care and treatment, including cancer care and treatment, cardiology treatment and care, orthopedics, birthing, and emergency medical services.

28. In the ordinary course of receiving treatment and health care services from VMMC, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Driver's license numbers;
- Financial account information;

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

- Payment card information;
- Medical histories;
- Treatment information;
- Medication or prescription information;
- Beneficiary information;
- Address, phone number, and email address, and;
- Health insurance information, including health insurance plan member IDs.

29. Prior to receiving care and treatment from VMMC, Plaintiff and Class Members were required to and did in fact turn over much (if not all) of the private and confidential information listed above.

30. Additionally, VMMC may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

31. VMMC also creates and maintains a considerable amount of Protected Health Information (PHI) in the course of providing medical care and treatment. This PHI includes billing account numbers, financial information, medical record numbers, dates of service, provider names, and medical and clinical treatment information regarding care received from VMMC.

32. On information and belief, VMMC provides each of its patients with a HIPAA compliant notice of its privacy practices (the "Privacy Notice") in respect to how they handle patients' sensitive and confidential information.

33. A copy of the Privacy Notice is maintained on VMMC's website, and may be found here: https://www.vmfh.org/content/dam/vmfhorg/pdf/virginia-mason-medical-center-privacy-

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

practices.pdf

34. Due to the highly sensitive and personal nature of the information VMMC acquires and stores with respect to its patients, VMMC recognizes patients' rights to privacy in its Privacy Notice, and promises in its Privacy Notice, to, among other things, maintain the privacy of patients' protected health information, which includes the types of data compromised in this Data Breach.

35. VMMC promises to maintain the confidentiality of patients' health, financial, and non-public personal information, ensure compliance with federal and state laws and regulations, and not to use or disclose patients' health information for any reasons other than those expressly listed in the Privacy Notice without written authorization.

36. As a condition of receiving medical care and treatment at Defendant's facilities, Defendant requires that its patients entrust it with highly sensitive personal information.

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

38. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members would not have entrusted VMMC with their Personal Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

39. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

THE ATTACK AND DATA BREACH

40. In January 2022, VMMC identified suspicious activity in its employee email network and determined that between December 21, 2021 and January 3, 2022 an unauthorized party had access to internal employee emails which allowed the attacker access to patients' and employees' Personal Information.

41. VMMC acknowledges that "[a]n unauthorized person may have accessed some of VMMC's staff email accounts between December 21, 2021 and January 3, 2022 through an email Phishing event."[1]

42. A phishing attack is a type of social engineering attack where the attacker impersonates a colleague or trusted source to encourage the recipient to download malicious software that allows the hacker to gain access to the company network. Phishing attacks are a common way for unauthorized individuals to gain access to company networks and retrieve sensitive data from those networks.[2]

43. VMMC further admits that the unauthorized party " An unauthorized person may have accessed some of VMMC's staff email accounts," and that " the information may have involved protected health information and employee information..."

44. VMMC further acknowledges that such information may include "name, address, date of birth, dates of service, medical record numbers, and clinical information about medical treatment or diagnoses [and] may have involved Social Security Number, passport information, driver's license, or health insurance number."

---

[1] https://www.vmfh.org/our-hospitals/virginia-mason-medical-center/patient-visitors/general-information/notice-of-vmmc-security-event

[2] https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-february-2018.pdf

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

45. On information and belief, the cybercriminals did in fact access VMMC files, and exfiltrate patient and employee PII and PHI during the roughly two weeks in which the cybercriminals had unfettered access to VMMC's email network.

46. On information and belief, the Private Information contained in the emails accessed by hackers was not encrypted.

47. On information and belief, the cyber-attack was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

48. On information and belief, the targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII and PHI of patients, like Plaintiff and the Class Members.

49. While VMMC stated in notice letters sent to Plaintiff and Class Members (as well as on its website) that it learned of the Ransomware Attack in January, 2022, VMMC did not begin notifying impacted patients, such as Plaintiff and Class Members, until May 26, 2022 – nearly six months after discovering the Data Breach.

50. Due to Defendant's inadequate security measures, Plaintiff and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

51. Plaintiff believes his Private Information was stolen in the attack and that said information was subsequently posted for sale on the dark web following the attack, as that is the modus operandi of all cybercriminals.

52. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

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

55. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.3 Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.4 The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.5 These incidents continue to rise in frequency, with an estimated 1,862 data breaches occurring in 2021.[6]

56. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic

---

[3] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed June 1, 2021)

[4] *Id.*

[5] *Id* at p15.

[6] https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

57. In 2021 alone there have been over 220 data breach incidents.[7] These approximately 220 data breach incidents have impacted nearly 15 million individuals.[8]

58. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

59. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[10]

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

This Email Phishing Attack Was Foreseeable.

---

[7] *See* Kim Delmonico, Another (!) Orthopedic Practice Reports Data Breach, Orthopedics This Week (May 24, 2021), https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/.

[8] *Id.*

[9] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited July 2, 2021).

[10] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

61. The targeted email phishing attack against Defendant was completely foreseeable. According to Verizon, over 90% of all cybersecurity attacks that result in a data breach start with a phishing attack.[11]

62. "Phishing is a cyber-attack that uses disguised email as a weapon. In simple terms, phishing is a method of obtaining personal information using deceptive e-mails and websites. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment."[12] The fake link will typically mimic a familiar website and require the input of credentials. Once input, the credentials are then used to gain unauthorized access into a system.

63. Phishing attacks are among the oldest, most common, and well-known form of cyberattack. "It's one of the oldest types of cyberattacks, dating back to the 1990s" and one that every organization with an internet presence is aware."[13] It remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[14]

64. Phishing attacks are well understood by the cyber-protection community and are generally preventable with the implementation of a variety of proactive measures such as

---

[11] *Verizon Says Phishing Drives 90% of Cybersecurity Breaches, Graphus* (Jan. 21, 2020), https://www.graphus.ai/verizon-says-phishing-still-drives-90-of-cybersecurity-breaches/

[12] Josh Fruhlinger, *What is Phishing? How This Cyber-Attack Works and How to Prevent It,* CSO Online (Sept. 4, 2020), https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

[13] *What is phishing? How this cyber attack works and how to prevent it, CSO Online, February 20, 2020,* https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (last visited October 28, 2020).

[14] *Phishing, Malwarebytes,* https://www.malwarebytes.com/phishing/ (last visited October 28, 2020).

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

sandboxing inbound e-mail[15], inspecting and analyzing web traffic, penetration testing[16], and employee education, among others.

65. As a sophisticated healthcare entity that collects and stores a particularly sensitive PII, an email phishing attack, and the potential harms arising therefrom, was reasonably foreseeable to Defendant.

66. Defendant Fails to Comply with FTC Guidelines

67. 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.

68. 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 patient 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

---

[15] Sandboxing is an automated process whereby e-mail with attachments and links are segregated to an isolated test environment, or a "sandbox," wherein a suspicious file or URL may be executed safely.

[16] Penetration testing is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit. The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incident. The primary goal of a penetration test is to identify weak spots in an organization's security posture, as well as measure the compliance of its security policy, test the staff's awareness of security issues and determine whether -- and how -- the organization would be subject to security disasters. See https://searchsecurity.techtarget.com/definition/penetration-testing (last visited October 28, 2020).

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

problems.17 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.[18]

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

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

71. These FTC enforcement actions include actions against healthcare providers 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

---

[17] *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 June 15, 2021).

[18] *Id.*

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

Section 5 of the FTC Act.")

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

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

74. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

75. As described above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

76. Several best practices have been identified that at a minimum should be implemented by healthcare providers like 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.

77. Other best cybersecurity practices that are standard in the healthcare 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.

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

78. 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.

79. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

80. Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

81. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information. And phishing is undoubtedly a well-known and common attack vector about which Defendant should have been aware and prepared to repel.

82. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Those safeguards must include physical, technical, educational, and administrative components.

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

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

84. A phishing attack such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

85. Phishing attacks are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> Regulated entities are required to ensure the integrity of ePHI by implementing "policies and procedures to protect ePHI from improper alteration or destruction." *See* 45 CFR 164.312(c)(1). In addition, the Security Rule requires regulated entities to assess and reduce risks and vulnerabilities to the availability of ePHI (as well as its confidentiality and integrity), which is defined as "the property that data or information is accessible and useable upon demand by an authorized person." *See* 45 CFR 164.308(a)(1)(ii)(A)-(B). Anti-phishing technologies can impede or deny the introduction of malware that may attempt to improperly alter, destroy, or block authorized access to ePHI (e.g., ransomware), and thus can be a helpful tool to preserve the integrity and availability of ePHI.[19]

86. Defendant's vulnerability to the phishing attack resulted from a combination of its own insufficiencies and failure to implement security awareness and training protocols, to encrypt sensitive, private, and protected information housed in its email system, implement access controls and authentication protocols, and implement anti-phishing technologies. That Defendant fell prey to a phishing attack and allowed unauthorized access to its email system for nearly two weeks

[19] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

demonstrates Defendant's failure to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

87. Defendant breached its obligations to Plaintiff and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. VMMC'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, cyber-attacks, hacking incidents, and ransomware attacks;

b. Failing to adequately protect patients' Private Information;

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

d. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

g. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

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

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

j. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

k. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

l. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

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

n. Failing to adhere to industry standards for cybersecurity.

88. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, VMMC negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

89. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased, and immediate risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

90. Hacking incidents and data breaches at medical facilities like VMMC are especially problematic because of the sensitive nature of the information at issue and the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

91. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[20]

92. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[21]

93. 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 will face "substantial costs and time to repair the damage to their good name and credit record."[22]

---

[20] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[21] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[22] *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.

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

94. 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.

95. 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.[23]

96. Identity thieves use stolen personal information such as Social Security numbers

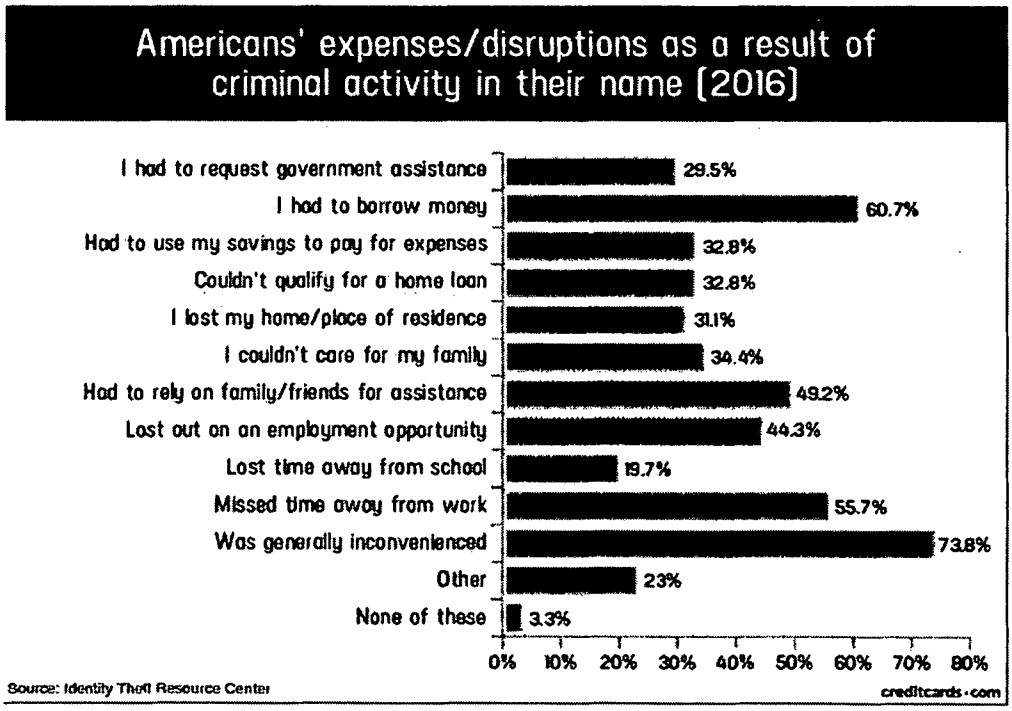
[23] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Mar. 16, 2021).

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

97. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

98. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[24]



[24] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

99. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[25]

100. 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.

101. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[26]

102. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

103. 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.

---

[25] 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).

[26] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Mar. 16, 2021).

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

104. 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.

105. 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.

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

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

108. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[27] 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.

109. For example, the Social Security Administration has warned that identity thieves

[27] *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/.

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

can use an individual's Social Security number to apply for additional credit lines.[28] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[29] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

110. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

111. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[30]

112. 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

---

[28] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 16, 2021).

[29] *Id* at 4.

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

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

10x on the black market."[31]

113. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[32]

114. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.
> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[33]

115. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[34] However, this is not the case. As

---

[31] 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.

[32] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021)

[33] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed July 20, 2021)

[34] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021)

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[35]

116. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[36]

117. Medical information is especially valuable to identity thieves.

118. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[37] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[38]

119. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

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

---

[35] *Id.*

[36] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021)

[37] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[38] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

that risk.

Plaintiff's and Class Members' Damages

121. To date, VMMC has done little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this data breach. Defendant's data breach notice letter completely downplays and disavows the theft of Plaintiff's and Class Members' Private Information, when the facts demonstrate that the Private Information was accessed and exfiltrated. The complimentary fraud and identity monitoring service offered by Defendant through Kroll is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiff's and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

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

123. Plaintiff Bergeson's Private Information (including without limitation his name, address, date of birth, Social Security number, email address, health insurance company and plan member ID, as well as information related to his COVID screening, vaccinations, and surveillance efforts) was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's IT network. Class Members' PII and PHI, as described above, was similarly compromised and is now in the hands of the same cyberthieves.

124. Plaintiff Bergeson is a former patient of Defendant.

125. Plaintiff Bergeson typically takes measures to protect his Private Information and is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

126. Plaintiff stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

127. To the best of his knowledge, Plaintiff's Private Information was never compromised in any other data breach.

128. Plaintiff 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, and similar identity theft.

129. Plaintiff 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 target such schemes more effectively to Plaintiff and Class Members.

130. Plaintiff and Class Members will also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

131. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by the hacker and cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

132. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of VMMC's computer

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

property and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

133. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial and medical accounts and records for misuse. Indeed, Defendant's own notice of data breach provides instructions to Plaintiff and Class Members about all the time that they will need to spend monitor their own accounts and statements received from healthcare providers and health insurance plans.

134. Plaintiff spent many hours over the course of several days attempting to verify the veracity of the notice of breach that he received and to monitor his financial and online accounts for evidence of fraudulent activities.

135. Plaintiff and Class Members have suffered 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. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

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

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

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

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

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

136. Moreover, Plaintiff 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 sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

137. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

138. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

139. Plaintiff bring this action on behalf of himself and on behalf of all other persons similarly situated.

140. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised in the Data Breach and were sent a notice of the Data Breach from Defendant. ("the Class").

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

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.

141. Numerosity - CR 23(a)(1). 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 reportedly include approximately 1.4 million patients and employees of Defendant SJ/C whose Private Information was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

142. Commonality - CR 23 (a)(2). 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 VMMC unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

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

c. Whether VMMC's data security systems prior to and during the hacking incident and Data Breach complied with applicable data security laws and regulations, *e.g.*, HIPAA;

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

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

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

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

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

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

i. Whether VMMC owed a duty to provide Plaintiff and Class Members notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of VMMC's misconduct;

k. Whether VMMC's conduct was negligent;

l. Whether VMMC's conduct was *per se* negligent;

m. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

n. Whether Defendant was unjustly enriched

o. Whether VMMC's conduct violated federal law;

p. Whether VMMC's conduct violated state law;

q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages.

143. Common sources of evidence may also be used to demonstrate VMMC's unlawful

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove VMMC's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

144. Typicality - CR 23 (a)(3). Plaintiff's claims are typical of the claims of the respective Class they seek to represent, in that the named Plaintiff and all Members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein.

145. Adequacy of Representation - CR 23 (a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff have no interests adverse to the interests of the other Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions, including data privacy litigation of this kind.

146. Predominance - CR 23 (b)(3). Defendant VMMC has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems 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.

147. Superiority - CR 23 (b)(3). 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

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

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.

148. VMMC has acted on grounds that apply generally to the Class as a whole, so that Class certification and the corresponding relief sought are appropriate on a Class-wide basis.

149. Likewise, particular issues under CR 23 (b)(4)(A) 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 Plaintiff 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 patient Private Information; and

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

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

150. 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
Violation of the Washington State Uniform Healthcare Information Act (RCW 70.02.005 *et seq.*) (On Behalf of Plaintiff and All Class Members)

151. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

152. Section 70.02.02 of the Revised Code of Washington provides that "Except as authorized elsewhere in this chapter, a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization. A disclosure made under a patient's written authorization must conform to the authorization."

153. At all relevant times, Defendant was a health care provider because it was authorized by the laws of Washington State to provide health care in the ordinary course of their business or practice. RCW 70.02.010(19).

154. At all relevant times, Defendant collected, stored, managed, and transmitted Plaintiff and Class Members' PII/PHI.

155. Plaintiff and Class Members PII/PHI is "Health Care Information" under RCW

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

70.02.010(17) in that it identifies or can be readily associated with the identify of a patient and directly relates to the patient's health care or that it is a required accounting of disclosures of health care information.

156. The Revised Code of Washington requires Defendant to implement and maintain standards of confidentiality with respect to all individually identifiable PHI disclosed to them and maintained by them. Specifically, RCW 70.20.020 prohibits Defendant from disclosing Plaintiff and Class Members' PHI without first obtaining their authorization to do so.

157. RCW 70.20.020-030 specifies the manner in which authorization must be obtained before PHI is released. Defendant, however, failed to obtain any authorization—let alone, proper authorization—from Plaintiff and Class Members before releasing and disclosing their PHI. As mandatorily required by RCW 70.20.150 (Security safeguards), Defendant also failed to effect reasonable safeguards for the security of all health care information they maintain, including but not limited to failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class Members' PHI. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff and Class Members' PHI was disclosed. By disclosing Plaintiff and Class Members' PHI without their written authorization. Defendant violated RCW 70.20.10 et seq., and its legal duty to protect the confidentiality of such information.

158. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violation of the RCW 70.20, pursuant to RCW 70.20.170, Plaintiff and Class

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

Members also are entitled to (1) injunctive relief; (2) actual damages per Plaintiff and each Class member, and; (3) reasonable attorneys' fees and all other expenses.

SECOND COUNT
Violation of the Washington State Consumer Protection Act
(RCW 19.86.010 *et seq.*)
(On Behalf of Plaintiff and All Class Members)

159. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

160. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

161. Defendant is a "person" as described in RWC 19.86.010(1).

162. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

163. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

164. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

Class Members' PII/PHI, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

165. Defendant also violated the CPA by failing to timely notify and concealing from Plaintiff and Class Members regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII/PHI, medical information, and identities.

166. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

167. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

168. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

medical fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or her PII/PHI; (5) deprivation of the value of his or her PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

169. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it.

170. Plaintiff, on behalf of himself and the Class Members also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, the Plaintiff, on behalf of himself and the Class Members requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

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

171. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

172. Plaintiff brings this claim individually and on behalf of the Class members.

173. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

174. Defendant had, and continue to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within their possession was compromised and precisely the type(s) of information that were compromised.

175. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

176. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like HIPPA and Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

178. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

179. 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.

180. 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.

181. Defendant systematically failed to provide adequate security for data in its possession.

182. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiff's and Class Members' Private Information;

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

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

d. Failure to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

183. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

184. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

185. Defendant, through its actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

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

187. It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

188. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

189. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding what type of Private Information has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

190. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

their Private Information.

191. As a result of Defendant's negligence and breach of duties, Plaintiff 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.

192. Plaintiff seeks the award of actual damages on behalf of the Class.

193. In failing to secure Plaintiff's and Class Members' Private Information and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

194. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Defendant to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

FOURTH COUNT
Negligence *per se*
(On Behalf of Plaintiff and All Class Members)

195. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

196. Pursuant to Section 5 of 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.

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

197. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

198. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

199. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

200. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

201. Plaintiff and Class Members are within the class of persons that the HIPAA was intended to protect.

202. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiff and the Class.

203. Defendant breached their duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA, by failing to provide fair, reasonable, or adequate computer

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

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

206. The injury and harm suffered by Plaintiff 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 and compromise of their Private Information.

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

FIFTH COUNT
Breach of Express Contract
(On Behalf of Plaintiff and All Class Members)

208. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

209. Plaintiff and Class Members entered into express contracts with Defendant that include Defendant's promise provide medical care and treatment, and the promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure. The express contract is embodied in the Privacy Notice and the Signed

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

Acknowledgment, and (upon information and belief) in other documents.

210. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and gave Defendant their Private Information (which also constitutes good and valuable consideration).

211. Defendant should have used some of Plaintiff's payments (or payments made on his behalf) to institute adequate protection of Plaintiff's Private Information, but Defendant did not.

212. As a result, Defendant exposed Plaintiff's Private Information during the Data Breach.

213. Plaintiff and Class Members thus paid Defendant for promised data security protections that they never received.

214. Had Plaintiff known of Defendant's substandard methods of protecting her Private Information, he would have sought medical care elsewhere.

215. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was accessed by unauthorized personnel as part of the Data Breach.

216. As a direct and proximate result of the breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries, and are entitled to actual, compensatory, and nominal damages.

SIXTH COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

217. Plaintiff repeats and re-alleges each and every factual allegation contained in all

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

previous paragraphs as if fully set forth herein.

218. Defendant provided Plaintiff and Class Members with an implied contract to protect and keep Defendant's patients' private, nonpublic personal, financial and health information when they gathered the information from each of their patients.

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

220. Defendant's agreement to reasonably protect such information included compliance with healthcare industry data security standards, and with applicable data security standards that govern healthcare entities like Defendant, including HIPAA.

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

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

223. HIPAA requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

224. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

225. Healthcare industry standards for data security include several best practices that

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

have been identified that a minimum should be implemented by healthcare providers like Defendant. These include, but are 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.

226. Other best cybersecurity practices that are standard in the healthcare 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.

227. Class Members who paid money to Defendant, or who had money paid on their behalf to Defendant, reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security that complied with healthcare industry data security standards and applicable regulations like HIPAA. Defendant failed to do so.

228. Plaintiff and Class Members would not have provided their personal, financial or health information to Defendant, but for Defendant's implied promises to safeguard and protect Defendant's patients' private personal, financial, and health information.

229. Plaintiff and Class Members performed their obligations under the implied contract when they provided their private personal, financial, and health information as a patient and when they paid for the services provided by Defendant.

230. Defendant breached the implied contracts with Plaintiff and Class Members by failing to protect and keep private the nonpublic personal, financial, and health information

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

provided to them about Plaintiff and Class Members.

231. As a direct and proximate result of Defendant's breach of their implied contracts, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

SEVENTH COUNT
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and All Class Members)

232. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

233. As a condition of their employment or status as a patient with Defendant, Plaintiff and the Class provided their personal and financial information. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

234. Defendant offered to provide goods and services to members of the Class who were patients in exchange for payment. Defendant also required the members of the Class who were patients to provide Defendant with their PII to receive services.

235. Class members who are employees accepted Defendant's offer of employment by providing their PII to Defendant.

236. Class members who are independent contractors accepted Defendant's provision of freight contracts by providing their PII to Defendant.

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

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

238. Had Plaintiff and Class Members known that Defendant would not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

239. VMMC represented to its patients and employees, implicitly and otherwise, that their PII would be secure. Plaintiff and members of the proposed Class relied on such representations when they agreed to provide their PII to VMMC. Plaintiff and the members of the Class would not have entrusted their PII to Defendant without such agreement with Defendant.

240. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

241. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

242. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

243. Defendant's duty to safeguard Plaintiff's and Class Member's PII is inherent in and consistent with the contracts entered into by VMMC and Plaintiff and Class Members.

244. Defendant would not have suffered harm by enacting industry standard measures

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

to safeguard Plaintiff's and Class Member's PII.

245. Defendant's failure to enact reasonable safeguards to protect the PII it collected resulted in harm to Plaintiff and Class Members and violated the covenant of good faith and fair dealing. Similarly, Defendant's failure to timely discover the breach, to timely notify affected persons, and to fully detail the scope of the breach in the "Notice of Data Security Incident," each suffices to demonstrate a breach of the covenant.

246. Plaintiff and Class Members have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

247. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract of good faith and fair dealing, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs in addition to all other damages or relief allowed by law.

EIGHTH COUNT
Breach of Confidence
(On Behalf of Plaintiff and All Class Members)

248. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

249. At all times during Plaintiff's and the Class's interactions with Defendant, Defendant were fully aware of the confidential and sensitive nature of Plaintiff's and the Class's PII and PHI that Plaintiff and the Class provided to Defendant.

250. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class's PII and PHI would be

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

251. Plaintiff and the Class provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

252. Plaintiff and the Class also provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

253. Defendant voluntarily received in confidence Plaintiff's and the Class's PII and PHI with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

254. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class's PII and PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class's confidence, and without their express permission.

255. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

256. But for Defendant's disclosure of Plaintiff's and the Class's PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and the Class's PII and PHI as well as the resulting damages.

257. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

result of Defendant's unauthorized disclosure of Plaintiff's and the Class's PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class's PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class's PII and PHI.

258. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of current and former patients and their beneficiaries and dependents; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

259. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm,

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

NINTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

260. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

261. This count is plead in the alternative to the breach of contract counts above.

262. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

263. As such, a portion of the payments made by or on behalf of Plaintiff 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.

264. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

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

266. In particular, Defendant enriched itself by saving the costs it reasonably should

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

267. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

268. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

269. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

270. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

271. Plaintiff and Class Members have no adequate remedy at law.

272. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts 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; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) 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 Plaintiff and Class Members.

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

274. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

TENTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All Class Members)

275. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

276. In light of the special relationships between Defendant and Plaintiff and Class Members, whereby Defendant became guardians of Plaintiff's and Class Members' Private

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members: (i) for the safeguarding of Plaintiff's and Class Members' Private Information; (ii) to timely notify Plaintiff and Class Members of a data breach and disclosure; and (iii) maintain complete and accurate records of what Private Information (and where) Defendant did and does store.

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

278. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

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

280. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

281. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

282. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

283. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

284. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

285. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

286. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

287. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

288. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized person(s) in violation of 45 C.F.R. § 164.502, et seq.

289. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

290. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

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

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

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on his own and behalf of all others similarly situated, pray for relief as follows:

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

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

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI 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 Plaintiff and the Class;

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN
227 W. MONROE STREET, STE. 2100
CHICAGO, IL 60606
PHONE: (866) 252-0878

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class Members;

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

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

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

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

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

RESPECTFULLY SUBMITTED this 13th day of June 2022.

FRANK FREED SUBIT & THOMAS LLP

By: */s/ Michael C. Subit*
Michael C. Subit, WSBA No. 29189
705 Second Avenue, Suite 1200
Seattle, Washington 98104-1798
(206) 682-6711 (phone)
(206) 682-0401 (fax)
Email: msubit@frankfreed.com

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

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW

Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
Email: dlietz@milberg.com

*pro hac vice to be filed

Attorneys for Plaintiff and the Proposed Class