UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

REGINALD SMITH, individually, and on behalf of all others similarly situated, **Plaintiff,** **v.** **THE MEDICAL COLLEGE OF WISCONSIN, INC.** **-and-** **PROGRESS SOFTWARE CORPORATION** **Defendants**	Civil Action No. 2:24-cv-1019 JURY DEMAND

CLASS ACTION COMPLAINT

Plaintiff, REGINALD SMITH (hereinafter, "Plaintiff"), individually, and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendants, THE MEDICAL COLLEGE OF WISCONSIN, INC. ("MCW") and PROGRESS SOFTWARE CORPORATION, ("PSC") (collectively, "Defendants") and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from Defendants' collective failures to safeguard the confidential personal information, Personally Identifying Information[1] ("PII") and Protected Health Information[2] ("PHI") (collectively, "PHI") of patients, including Plaintiff and the proposed

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and

Class Members, resulting in the unauthorized disclosure of that PHI in May 2023 in a cyberattack to the MOVEit Transfer tool of PSC (the "Data Breach").[3]

2. On information and belief, the PHI compromised in the Data Breach includes Plaintiff's and the Class's names, Social Security numbers, dates of birth, health insurance applications and/or claim information, medical history, conditions, treatments and/or diagnosis information, medical procedure information, patient dates of service, and patient medical record numbers.[4]

3. MCW is a private medical college which provides primary and specialty medical treatment services at hospitals and clinics in the Milwaukee area and eastern Wisconsin."[5]

4. PSC is a software company offering a range of products and services to government and corporate entities across the country and around the world, including cloud hosting and secure file transfer services such as MOVEit file transfer tool and MOVEit cloud.

5. This Data Breach differs from typical data breaches because it affects patients who had no relationship with PSC, never sought one, and never consented to PSC collecting and storing

---

its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). MCW is clearly a "covered entity" and some of the data compromised in the Data Breach is "protected health information," subject to HIPAA.

[3] *See Notice of Security Incident,* November 14, 2023, **(hereinafter "Data Breach Notice") attached as Exhibit A**.

[4] *Id*.

[5] https://www.mcw.edu/patient-care/hospitals-and-clinics (last accessed Apr. 17, 2024).

their information.

6. PSC sourced their information from third parties, such as MCW, stored it on PSC's systems, and assumed a duty to protect it, advertising that it "put in place physical, electronic, and managerial procedures designed to help prevent unauthorized access, to maintain data security, and to use correctly the Information we collect online."[6] But PSC never implemented the security safeguards needed despite acknowledging their importance.

7. MCW utilized PSC's MOVEit Transfer solution to store it patients' PHI which had been entrusted to it by Plaintiff and the Class.

8. On information and belief, PSC was notified of a system vulnerability in its MOVEit cloud on May 28, 2023.[7]

9. On or about May 31, 2023, PSC posted a notice on its website confirming a recently discovered SQL injection vulnerability related to its MOVEit Transfer and MOVEit Cloud file transfer services resulting from a breach in its network and systems that may have been exploited by cybercriminals from as far back as 2021.[8]

10. At an unknown time, MCW was alerted to the MOVEit Data Breach, and following an investigation, on September 21, 2023 discovered that "certain files containing [patients'] personal information were potentially removed from our MOVEit server by an unauthorized party on May 27, 2023."[9]

---

[6] *Privacy Policy*, PSC, https://www.progress.com/legal/privacy-policy (last visited June 21, 2023).
[7] Hackers use flaw in popular file transfer tool to steal data, Reuters, https://www.reuters.com/technology/hackers-use-flaw-popular-file-transfer-tool-steal-data-researchers-say-2023-06-02/ (last visited June 21, 2023).
[8] See https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
[9] *See Data Breach Notice*, Exhibit A.

11. Despite the enormity of the breach, PSC has not yet began sent direct notice to those impacted by the Data Breach, though many of its customers—like MCW—have begun notifying individuals, including Plaintiff, that their PHI has been compromised as a result of the PSC Data Breach.[10]

12. PSC continues to delay notification of the Data Breach to its victims even though Plaintiff and approximately 60 million Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

13. PSC is actively obfuscating the breach details, nature of the breach and the threat it posted—refusing to tell its consumers who are impacted, how many people were impacted, how the breach happened, or why PSC has delayed notifying its victims that hackers had gained access to highly sensitive PHI.

14. Defendants' failure to timely detect and report the Data Breach made its patients vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PHI.

15. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PHI misuse.

16. In failing to adequately protect Plaintiff's and the Class's PHI, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendants breached their duties to Plaintiff and the Class and violated state and federal law, harming an unknown

[10] *Id.*

number of individuals who entrusted MCW with their PHI.

17. Plaintiff and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted MCW with their PHI which MCW gave to PSC as stored in the MOVEit Transfer solutions tool. But Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent the Data Breach.

18. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this action seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

19. The exposure of one's PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, consumers' and patients' private information was exactly that—private. Not anymore. Now, Plaintiff's and the Class's PHI is forever exposed and unsecure.

PARTIES

20. Plaintiff is a natural person, and resident and citizen of the State of Wisconsin, residing in Milwaukee, Wisconsin where he intends to remain. Plaintiff received treatment from MCW and received MCW's Data Breach Notice notifying him that his PHI was compromised in the Data Breach.

21. Defendant, MCW, is a corporation organized and existing under the laws of the State of Wisconsin with its principal place of business at 8701 Watertown Plank Road, Milwaukee, Wisconsin 53226

22. Defendant, PSC, is a corporation organized and existing under the laws of the State of Massachusetts with its principal place of business at 15 Wayside Road, Suite 400, Burlington,

Massachusetts 01803.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. Plaintiff and PSC are citizens of different states.

24. This Court has personal jurisdiction over Defendants MCW because MCW maintains its principal place of business in this District and does substantial business in this District.

25. This Court has personal jurisdiction over Defendants PSC because PSC does substantial business in this District.

26. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF COMMON FACTS

A. Defendant MCW

27. MCW is the "third largest private medical school in the nation," and provides medical care and treatment to patients in Milwaukee and Eastern Wisconsin, with 1,780 physicians, 905 advanced practice providers, and which treats 5.1 million patients each year.[11]

28. MCW boasts that, "[a]cademic medicine brings the best medical education, research and patient care together to transform the practice of medicine. The resulting synergy is what sets the Medical College of Wisconsin apart…"[12]

[11] MCW Impact Sheet 2023, avail. at https://www.mcw.edu/-/media/MCW/About-MCW/Facts-and-Impact/MCW-Impact-Sheet-2023.pdf (last acc. Apr. 17, 2024).
[12] https://www.mcw.edu/patient-care (last acc. Apr. 17, 2024).

29. MCW "provide[s] primary and specialty care at many hospitals and clinics in metro Milwaukee and eastern Wisconsin. You can find our physicians and health care providers at Froedtert Hospital, Children's Wisconsin, and the Clement J. Zablocki VA Medical Center."[13]

30. MCW generates annual revenue approximating $1.4 Billion.[14]

31. As part of its business and as a condition of providing treatment, MCW requires that its patients provide MCW with their PHI, including their names, Social Security numbers, dates of birth, health insurance applications and/or claim information, medical history, conditions, treatments and/or diagnosis information, medical procedure information, patient dates of service, and patient medical record numbers.

32. In collecting and maintaining PHI, MCW agreed it would safeguard the PHI in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PHI.

33. In fact, MCW maintains privacy policies, such as the Notice of Privacy Practices for MCW clinics, in which it promises that, "[w]e are committed to the privacy of your PHI, and we comply with applicable law and accreditation standards regarding patient privacy."[15]

34. MCW utilizes PSC's MOVEit Transfer tool, on information and belief, to store patients' PHI.

35. Despite recognizing its duty to do so, on information and belief, MCW failed to implement or failed to ensure that PSC implemented reasonably cybersecurity safeguards or

[13] https://www.mcw.edu/patient-care/hospitals-and-clinics (last acc. Apr. 17, 2024).
[14] https://www.zoominfo.com/c/medical-college-of-wisconsin/24363744 (last acc. Apr. 17, 2024).
[15] *Notice of Privacy Practices*, effective April 14, 2003, last revised Oct. 25, 2019, avail. at https://www.mcw.edu/-/media/MCW/Departments/Corporate-Compliance/MCW-Notice-of-Privacy-Practices.pdf (last acc. Apr. 17, 2024).

policies to protect its patients' PHI or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, there were significant vulnerabilities in MCW's systems for cybercriminals to exploit and gain access to consumers' PHI.

B. Defendant PSC

36. PSC considers itself "the experienced, trusted provider of products designed with you, our customers, in mind", boasting that one of its values is to "uphold trust" of its clients and consumers.[16] PSC touts a total annual revenue of 602 million.[17]

37. As part of its business, PSC receives and maintains the PHI of thousands of consumers (such as, *inter alia*, its clients' consumers) In collecting and maintaining PHI, PSC agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PHI.

38. Indeed, PSC boasts that it "employs industry standard security measures to ensure the security of information" that it collects, promising that "any Personal Information about you that we handle will only be accessible by those Progress personnel who have a reason to do so."[18]

39. In collecting and maintaining consumers' PHI, PSC agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PHI.

40. Despite recognizing its duty to do so, on information and belief, PSC has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' PHI or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its

[16] About, Progress, https://www.progress.com/company (last visited June 21, 2023).
[17] PSC Revenue, Zippia, https://www.zippia.com/progress-software-careers-9392/revenue/ (last visited June 21, 2023).
[18] *Privacy Policy, PSC*, https://www.progress.com/legal/privacy-policy (last visited June 21, 2023).

systems. As a result, PSC leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PHI.

C. The Data Breach

41. Plaintiff and the proposed Class Members provided their PHI to MCW and other entities which utilized PSC's MOVEit Transfer tool and thus transferred that PHI to PSC.

42. According to its web page regarding MOVEit Transfer and MOVEit Cloud Vulnerability, PSC discovered "a vulnerability in MOVEit Transfer and MOVEit Cloud (CVE-2023-34362) that could lead to escalated privileges and potential unauthorized access to the environment" on May 31, 2023. Following an internal investigation, PSC discovered "additional vulnerabilities that could potentially be used by a bad actor to stage an exploit. These newly discovered vulnerabilities are distinct from the previously reported vulnerability shared on May 31, 2023".[19]

43. In other words, PSC's investigation revealed that its cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its consumers' highly sensitive PHI.

44. On information and belief, the notorious Clop ransomware gang claimed responsibility for the cyberattack, exploiting the MOVEit Transfer and MOVEit Cloud vulnerability for nefarious purposes. Clop is one of the most active ransomware actors, having breached over 130 organizations alone through a similar file transfer tool vulnerability.[20] PSC, a

[19] MOVEit Transfer and MOVEit Cloud Vulnerability, Progress Security Center, https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability (last visited June 21, 2023).

[20] Clop ransomware hack of Fortra GoAnywhere MFT hits 1M CHS patients, SC Medica, https://www.scmagazine.com/news/ransomware/clop-ransomware-hack-of-fortra-goanywhere-mft-hits-1m-chs-patients (last visited June 21, 2023).

"leading" software company providing file transfer services, knew or should have known of the tactics that groups like Clop employ.

45. With the PHI secured and stolen by Clop, the hackers then purportedly issued a ransom demand to PSC. However, PSC has provided no public information on the ransom demand or payment.

46. On information and belief, Clop threatened to name all companies whose customers' PHI was stolen in the Data Breach, stating that names would be added to their data leak site on June 14 if negotiations did not occur. Additionally, Clop stated that if the extortion demand is not paid, it would begin leaking all data obtained in the Data Breach, including PHI onto its site on June 21st.[21]

47. PSC continues to delay notifying its victims about the Data Breach, despite Clop's threat to leak the PHI it obtained through the Data Breach onto the dark web. To date, PSC has not yet begun sending out Data Breach Notices.

48. PSC kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

49. In response to the Data Breach, PSC contends that it has or will be making "[a new] upgrade and migration guide", "new indicators of compromise", as well as "enhanced remediation steps".[22] Although PSC fails to expand on what these alleged enhancements and "steps" are, such enhancements should have been in place before the Data Breach.

---

[21] Clop ransomware gang starts extorting MOVEit data-theft victims, bleeping computer, https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-starts-extorting-moveit-data-theft-victims/ (last visited June 21, 2023).

[22] MOVEit Transfer Critical Vulnerability, Progress Commuinity, https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 (last visited June 21, 2023).

50. Through its Breach Notice, PSC also recognized the actual imminent harm and injury that flowed from the Data Breach, encouraging that it "is extremely important that [clients and consumers] take immediate action"[23]

51. According to MCW, as communicated in its Data Breach Notice, at an unstated time, it received notice from one of its unnamed "third-party vendors," on information and belief PSC, regarding the MOVEit Transfer solution vulnerability "which has been actively exploited by unauthorized actors to gain access to data stored on the MOVEit server."[24]

52. As MCW went onto state, "MOVEit has acknowledged the vulnerability and has since provided patches to remediate the exploit. There was no compromise of MCW's broader network security."[25]

53. Following being alerted of the breach, according to MCW, it "immediately took actions to mitigate and assess the scope of information potentially compromised" with the assistance of third party-professionals, and by September 21, 2023 confirmed that "certain files containing [patients'] personal information were potentially removed from our MOVEit server by an unauthorized party on May 27, 2023."[26]

54. According to MCW, the PHI of its patients compromised and unauthorizedly disclosed in the Data Breach includes names, Social Security numbers, dates of birth, health insurance applications and/or claim information, medical history, conditions, treatments and/or diagnosis information, medical procedure information, patient dates of service, and patient medical record numbers.[27]

---

[23] *Id*.
[24] *See Data Breach Notice*, Exhibit A.
[25] *Id.*
[26] *Id.*
[27] *Id.*

55. MCW encouraged Data Breach victims to vigilantly monitor their financial account statements and credit reports for fraudulent activity, and recommended that they place fraud alerts and credit freezes on their credit files.[28]

56. Furthermore, MCW offered Data Breach victims 12-months of Experian IdentityWorks protection which it recommended they accept.

57. MCW likewise encouraged Data Breach victims to take general measures to protect their medical information from identity theft:

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.[29]

58. At the same time, MCW obfuscated the nature and severity of the breach, failing to inform Data Breach victims of the name of the third-party vendor, and stating that it "is not aware of any reports of identity fraud or financial fraud for any information as a direct result of this incident."[30]

59. At this stage, according to the Wisconsin Department of Agriculture, Trade and Consumer Protection, the MOVEit Data Breach has impacted approximately 1,100 business

[28] *Id.*
[29] *Id.*
[30] *Id.*

customers of PSC, like MCW, and impacted 60 million individuals.[31]

60. Despite their duties and alleged commitments to safeguard PHI, Defendants failed to take adequate measures to protect the vast amounts of patient PHI they collected and stored on the MOVEit software, including failing to follow industry standard practices, and failing to ensure that vendors undertook such measures, failing to adequately train and supervise information technology (IT) and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, failing to warn Plaintiff and Class Members of Defendants' inadequate data security practices, failing to encrypt or adequately encrypt the PHI, and otherwise failing to secure the software and hardware using reasonable and effective data security procedures, resulting in the Data Breach.

61. Indeed, the PHI was maintained on computer systems and networks that utilized PSC's MOVEit tool, which contained security vulnerabilities which were exploited in this Data Breach. MCW and others utilized PSC's MOVEit software tool to store PHI despite these security vulnerabilities.

62. As a result of the Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their dates of birth and Social Security numbers. Accordingly, any credit monitoring and identity theft protection which MCW offered is wholly insufficient to compensate Plaintiff and the Class Members for their damages resulting from the Data Breach.

63. As a result of the Data Breach which Defendants permitted to occur by virtue of their inadequate data security practices, Plaintiff and the proposed Class Members have suffered

[31] Wisconsin Department of Agriculture, Trade and Consumer Protection, *Data Breach Archive*, avail. at https://datcp.wi.gov/Pages/Programs_Services/DataBreachArchive.aspx (last acc. Apr. 17, 2024).

injury and damages, as set forth herein.

D. The Data Breach was a Foreseeable Risk of which Defendants Were on Notice.

64. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the file-transfer software industry preceding the date of the breach, including recent similar attacks against secure file transfer companies like Accellion and Fortra carried out by the same Russian cyber gang, Clop.[32]

65. In light of recent high profile data breaches at other file-transfer software companies, Defendants knew or should have known that their electronic records and servers and patients' and others' PHI would be targeted by cybercriminals.

66. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[33] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[34]

67. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PHI." The FBI further warned that that "the increasing sophistication of cyber criminals

---

[32] *See* https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomwaregang/ (last visited on June 21, 2023); see also https://www.bleepingcomputer.com/news/security/fortra-sharesfindings-on-goanywhere-mft-zero-day-attacks/ (last visited on June 21, 2023).

[33] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 13, 2023).

[34] *Id*.

will no doubt lead to an escalation in cybercrime." [35]

68. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including PSC.

E. Plaintiff's Experience

69. Plaintiff is a patient of MCW, receiving medical treatment from MCW in Milwaukee, Wisconsin at Froedtert Hospital and other MCW clinics.

70. As a condition of receiving treatment from MCW, Plaintiff provided MCW with his sensitive, private, PHI, including his name, date of birth, Social Security number, medical information and insurance information.

71. At all times, Plaintiff carefully guards the privacy of his PHI, maintaining it in a secure manner, and never knowingly transmitting unencrypted sensitive PHI over the internet or any other unsecured source.

72. To his knowledge, Plaintiff has never had his PHI compromised in a data security breach prior to the instant Data Breach.

73. Plaintiff received MCW's Data Breach Notice dated November 14, 2023 informing him that his name, Social Security number, date of birth, health insurance application and/or claim information, medical history, condition, treatment and/or diagnosis information, medical procedure information, patient dates of service, and patient medical record number were compromised and potentially removed in the Data Breach.

74. On information and belief, Plaintiff's above PHI was actually unauthorizedly disclosed to cybercriminals in the Data Breach.

[35] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited June 13, 2023).

75. As a direct and proximate result of the Data Breach, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, including fraudulent misuse of his PHI by cybercriminals.

76. Indeed, following the Data Breach, unknown criminals utilized Plaintiff's PHI disclosed in the breach to attempt to obtain credit and loans in Plaintiff's name, as evidenced by rejection letters he received from banks and/or loan companies concerning loans Plaintiff did not apply for.

77. Based on the occurrence of this fraud, on information and belief, his PHI compromised in this Data Breach has been posted to the Dark Web for sale and fraudulent misuse.

78. Further, as a result of the Data Breach, Plaintiff has spent time, and will be required to spend time in the future, dealing with the consequences of the Data Breach, including time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred, and time addressing fraudulent misuse of his PHI disclosed in the Data Breach. This time has been lost forever and cannot be recaptured.

79. Plaintiff will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft.

80. Plaintiff fears for his personal financial security and uncertainty over what PHI was exposed in the Data Breach, and has experienced feelings of emotional distress, anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

81. Moreover, Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI—a form of intangible property that Plaintiff entrusted to Defendants,

which was compromised in and as a result of the Data Breach.

82. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PHI being placed in the hands of unauthorized third parties and possibly criminals.

83. Plaintiff has a continuing interest in ensuring that his PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

F. Plaintiff and the Proposed Class Have Suffered Injury and Damages Due to the Data Breach

84. Plaintiff and members of the proposed Class have suffered injury and damages from the misuse of their PHI that can be directly traced to Defendants.

85. As a result of Defendants' failures to prevent the Data Breach, Plaintiff and the proposed Class have suffered, and will continue to suffer and damages, including unauthorized disclosure of this PHI, monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. Fraudulent misuse of PHI to attempt to obtain credit and loans;

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

c. The diminution in value of their PHI;

d. The compromise and continuing publication of their PHI;

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

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent

researching how to prevent, detect, contest, and recover from identity theft and fraud;

g. Delay in receipt of tax refund monies;

h. Unauthorized use of stolen PHI;

i. Emotional distress;

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

86. Further, as a result of the Data Breach, Plaintiff and the Class are at an increased risk of further identity theft and fraud as the PHI remains in the hands of cybercriminals.

87. Stolen PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI can be worth up to $1,000.00 depending on the type of information obtained.

88. The value of Plaintiff's and the Class's PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen PHI openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

89. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

90. One such example of criminals using PHI for profit is the development of "Fullz" packages.

91. Cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of

accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

92. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

93. Defendants disclosed the PHI of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PHI of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PHI.

94. Defendants' failures to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

G. Defendants failed to adhere to FTC guidelines.

95. According to the Federal Trade Commission ("FTC"), the need for data security

should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of PHI.

96. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PHI that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

97. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

98. The FTC recommends that companies not maintain information 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.

99. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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.

100. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

H. Defendants Fail to Comply with Industry Standards

101. As noted above, experts studying cyber security routinely identify entities in possession of PHI as being particularly vulnerable to cyberattacks because of the value of the PHI which they collect and maintain.

102. Several best practices have been identified that a minimum should be implemented by businesses in possession of PHI, like Defendants, 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. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

103. Other best cybersecurity practices that are standard for businesses 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. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

104. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

105. These foregoing frameworks are existing and applicable industry standards for healthcare provider's or other business's obligations to provide adequate data security for its patients. Upon information and belief, Defendants failed to comply with at least one, or all, of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

I. Defendants' Conduct Violates HIPAA and Evidences Their Insufficient Data Security

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

107. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of sensitive patient health information. Safeguards must include physical, technical, and administrative components.

108. 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 PHI like the data Defendants left unguarded. HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules 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).

109. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

110. Defendants breached their obligations to Plaintiff and the Class Members and/or

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

a. Failing to adequately protect patients' PHI;

b. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

c. Failing to practice the principle of least-privilege and maintain credential hygiene;

d. Failing to avoid the use of domain-wide, admin-level service accounts;

e. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

f. 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);

g. 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);

h. 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);

i. 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);

j. 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); and/or

k. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI/ 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 (definition of encryption).

111. As the result of Defendants' violations, Defendants negligently and unlawfully failed to safeguard Plaintiff's and the Class Members' PHI.

CLASS ACTION ALLEGATIONS

112. Plaintiff sues on behalf of himself and all others similarly situated, the proposed Class, defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **All individuals residing in the United States whose PHI was compromised, unauthorizedly accessed, or removed in the PSC Data Breach and MOVEit vulnerability ("the Class").**

113. Further, Plaintiff proposes an MCW Subclass, defined as follows:

> **All individuals residing in the United States whose PHI was maintained by MCW and compromised, unauthorizedly accessed, or removed in the PSC Data Breach and MOVEit vulnerability ("MCW Subclass").**

114. Excluded from the Class and Subclass are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of

Defendants' officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

115. Plaintiff reserves the right to amend the class definition.

116. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

117. **Numerosity, Fed. R. Civ. P. 23(a)(1):** Plaintiff is representative of the Class, consisting of at least 6 million members, far too many to join in a single action.

118. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control.

119. **Typicality, Fed. R. Civ. P. 23(a)(3)** Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

120. **Adequacy, Fed. R. Civ. P. 23(a)(4)**: Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

121. **Commonality, Fed. R. Civ. P. 23(a)(2) and Fed. R. Civ. P. 23 (b)(3):** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

a. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PHI;

b. Whether Defendants failed to implement and maintain reasonable security

procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants were negligent in maintaining, protecting, and securing PHI;

d. Whether Defendants breached contractual promises to safeguard Plaintiff's and the Class's PHI;

e. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether Defendants' Data Breach Notices were reasonable;

g. Whether the Data Breach caused Plaintiff's and the Class's injuries;

h. What the proper damages measure is; and

i. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

122. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class Against All Defendants)

123. Plaintiff realleges and reincorporates the preceding paragraphs as if fully set forth herein.

124. Plaintiff and members of the Class entrusted their PHI to Defendants. Defendants owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PHI in

their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

125. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failures to adequately safeguard their PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PHI —just like the Data Breach that ultimately came to pass.

126. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's PHI by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

127. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PHI. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

128. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and the Class's PHI.

129. The risk that unauthorized persons would attempt to gain access to the PHI and

misuse it was foreseeable. Given that Defendants holds vast amounts of PHI, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PHI — whether by exploitation of software vulnerabilities, malware, ransomware, or otherwise.

130. PHI is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PHI of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

131. Defendants breached their duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PHI of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact.

132. As a direct and proximate result of Defendants' negligence and/or negligent supervision, Plaintiff and the Class have suffered or will imminently suffer actual, tangible, injury-in-fact and damages, including, without limitation: monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress; fraudulent misuse of PHI to attempt to obtain credit and loans; loss of the opportunity to control how their PHI is used; diminution in value of their PHI; compromise and continuing publication of their PHI; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover

from identity theft and fraud; delay in receipt of tax refund monies; other unauthorized use of stolen PHI; the continued risk to their PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PHI in their possession.

133. As a result, Plaintiff and the Class Members are entitled to recover actual and compensatory damages in an amount to be proven at trial, and punitive damages.

134. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) properly notify affected victims of the Data Breach, (ii) strengthen their data security systems and monitoring procedures; and (iii) submit to future annual audits of those systems and monitoring procedures.

135. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the continuing unauthorized disclosure of the PHI of Plaintiff and the Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class Against All Defendants)

136. Plaintiff realleges and reincorporates the preceding paragraphs as if fully set forth herein.

137. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PHI.

138. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers or, in this case, patients' PHI. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the members of the Class's PHI.

139. Defendants breached their duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PHI.

140. Further, pursuant to HIPAA, 42 U.S.C. § 1301, *et seq*., and implementing regulations and rules, the HIPAA Security Rule, covered entities are required to: ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted (45 C.F.R. § 164.306(a)(1)); 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 (45 C.F.R. § 164.312(a)(1)); implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports (45 C.F.R. § 164.308(a)(1)(ii)(D)); protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI (45 C.F.R. § 164.306(a)(2)); protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information (45 C.F.R. § 164.306(a)(3)); render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, by encrypting 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).

141. On information and belief, Defendants failed to comply with the foregoing provisions of HIPAA, the Security Rule, 45 C.F.R. § 164.306(a)(1), 45 C.F.R. § 164.312(a)(1), 45 C.F.R. § 164.308(a)(1)(ii)(D), 45 C.F.R. § 164.306(a)(2), 45 C.F.R. § 164.306(a)(3), and 45 CFR § 164.304.

142. Defendants' duties to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PHI.

143. Defendants violated their duties under Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Plaintiff's and the Class's PHI and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PHI Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

144. The harm that has occurred is the type of harm the FTC Act and HIPAA are intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because 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.

145. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

146. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members

of the Class to suffer the foreseeable harms associated with the exposure of their PHI.

147. Had Plaintiff and the Class known that Defendants did not adequately protect their PHI, Plaintiff and members of the Class would not have entrusted Defendants with their PHI.

148. Defendants' various violations and their failures to comply with applicable laws and regulations constitutes negligence *per se*.

149. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered or will imminently suffer actual, tangible, injury-in-fact and damages, including, without limitation: monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress; fraudulent misuse of PHI to attempt to obtain credit and loans; loss of the opportunity to control how their PHI is used; diminution in value of their PHI; compromise and continuing publication of their PHI; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; other unauthorized use of stolen PHI; and the continued risk to their PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PHI in their possession.

150. As a result, Plaintiff and the Class Members are entitled to recover actual and compensatory damages in an amount to be proven at trial, and punitive damages.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the MCW Subclass Against MCW)

151. Plaintiff realleges and reincorporates the preceding paragraphs as if fully set forth herein.

152. Defendant offered to provide medical services to Plaintiff and the MCW Subclass Members in exchange for payment, a portion of which was paid for adequate data security, and in exchange for the MCW Subclass Members' PHI, which MCW required as a condition of rendering treatment.

153. In turn, MCW impliedly promised to protect Plaintiff's and the MCW Subclass Members' PHI through adequate data security measures as manifested by MCW's conduct, and representations, including those found in MCW's Notice of Privacy Practices that it is "committed to the protection of patient health information in accordance with applicable law and accreditation standards regarding patient privacy."[36]

154. Plaintiff and the members of the MCW Subclass accepted Defendant's offer by providing PHI to MCW in exchange for receiving MCW's medical services, and then by paying for and receiving the care.

155. The valid and enforceable implied contracts that Plaintiff and MCW Subclass Members entered into with MCW included MCW's promise to protect nonpublic PHI given to MCW from unauthorized disclosures. Plaintiff and MCW Subclass Members provided their PHI to MCW in reliance of that promise.

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

[36] *See Notice of Privacy Practices*, avail. at https://www.mcw.edu/-/media/MCW/Departments/Corporate-Compliance/MCW-Notice-of-Privacy-Practices.pdf

157. Plaintiff and MCW Subclass Members reasonably believed and expected that MCW would adequately employ adequate data security to protect that PHI, and ensure that MCW's vendors to whom MCW gave Plaintiff's and the MCW Subclass Members' PHI employed adequate data security to protect that PHI. MCW failed to do so.

158. Under the implied contracts, MCW promised and was obligated to: (a) provide medical services to Plaintiff and MCW Subclass Members; and (b) protect Plaintiff's and the MCW Subclass Members' PHI and ensure that its vendors protected Plaintiff's and the Class Members' PHI: (i) provided to obtain such services and/or (ii) created in connection therewith. In exchange, Plaintiff and MCW Subclass Members agreed to pay money for these services and to turn over their PHI to MCW.

159. Both the provision of these medical services, and the protection of Plaintiff's and MCW Subclass Members' PHI, including through MCW's vendors, were material aspects of these implied contracts.

160. Plaintiff and MCW Subclass Members would not have entrusted their PHI to MCW and entered into these implied contracts with MCW without an understanding that their PHI would be safeguarded and protected, or entrusted their PHI to MCW in the absence of its implied promise to monitor their or their vendor's computer systems and networks to ensure that PHI was not disclosed to unauthorized parties and exposed to the public as occurred in the Data Breach.

161. A meeting of the minds occurred when Plaintiff and the MCW Subclass Members agreed to, and did, provide their PHI to MCW and paid for services for, amongst other things, (a) the provision of such services and (b) the protection of their PHI.

162. Plaintiff and the MCW Subclass Members performed their obligations under the contracts when they paid for services, and provided their PHI, to MCW.

163. MCW materially breached its contractual obligations to protect the nonpublic PHI of Plaintiff and the MCW Subclass Members and to ensure that its vendors protected their nonpublic PHI which MCW required and gathered, and then gave to its vendor, when the information was unauthorized disclosed in the Data Breach.

164. 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.

165. 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.

166. MCW's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

167. The Data Breach was a reasonably foreseeable consequence of MCW's conduct, by acts of omission or commission, in breach of these contracts, including failing to adequately safeguard PHI and failing to supervise its vendors to whom MCW gave its customers' PHI.

168. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, including failing to supervise its vendors for the protection of PHI, Plaintiff and MCW Subclass Members did not receive the full benefit of their bargains, and instead received services that were of a diminished value compared to those described in the contracts.

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

170. As a direct and proximate result of MCW's breach of implied contract, including breach of the implied covenant of good faith and fair dealing, Plaintiff and the MCW Subclass have suffered or will imminently suffer actual, tangible, injury-in-fact and damages, including, without limitation: monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress; fraudulent misuse of PHI to attempt to obtain credit and loans; loss of the opportunity to control how their PHI is used; diminution in value of their PHI; compromise and continuing publication of their PHI; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; other unauthorized use of stolen PHI; and the continued risk to their PHI, which remains in MCW's possession and is subject to further breaches so long as MCW fails to undertake the appropriate measures to protect the PHI in its possession.

171. Plaintiff and the MCW Subclass Members are entitled to actual, compensatory and consequential, and nominal damages suffered as a result of MCW's breach of implied contract.

COUNT IV
BREACH OF THIRD PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class Against PSC)

172. Plaintiff realleges and reincorporates the preceding paragraphs as if fully set forth herein.

173. On information and belief, PSC entered into contracts with its government and corporate customers, including MCW, to provide MOVEit secure file transfer services, which included data security practices, procedures, and protocols sufficient to safeguard the PHI that was entrusted to it.

174. These contracts were made expressly for the benefit of Plaintiff and the Class, as it was their PHI that Defendants agreed to receive, store, utilize, transfer, and protect through its services. The benefit of collection and protection of the PHI of Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

175. PSC knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class Members would be harmed.

176. PSC breached its contracts with customers by, among other things, failing to adequately secure Plaintiff's and Class Members' PHI.

177. As a direct and proximate result, Plaintiff and the Class have suffered or will imminently suffer actual, tangible, injury-in-fact and damages, including, without limitation: monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress; fraudulent misuse of PHI to attempt to obtain credit and loans; loss of the opportunity to control how their PHI is used; diminution in value of their PHI; compromise and continuing publication of their PHI; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax

refund monies; other unauthorized use of stolen PHI; and the continued risk to their PHI, which remains in MCW's possession and is subject to further breaches so long as PSC fails to undertake the appropriate measures to protect the PHI in its possession.

178. Plaintiff and the Class Members are entitled to actual, compensatory and consequential, and nominal damages suffered as a result of PSC's breach.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class Against All Defendants)

179. Plaintiff realleges and reincorporates the preceding paragraphs as if fully set forth herein.

180. This claim is brought in the alternate to Plaintiff's breach of implied contract and breach of third-party beneficiary contract claims.

181. Plaintiff and Class members conferred a monetary benefit upon Defendants by providing Defendants with their PHI. After all, Defendants benefitted from using their PHI to provide medical services and/or file transferring software services.

182. Defendants appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendants benefited from receiving Plaintiff's and Class members' PHI, as this was used to provide medical services and/or file transferring software services.

183. Plaintiff and Class Members reasonably understood that Defendants would use adequate cybersecurity measures to protect the PHI that they were required to provide based on Defendants' duties under state and federal law and its internal policies.

184. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PHI.

185. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendants instead calculated to avoid their data security

obligations 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 Defendants' failures to provide the requisite security.

186. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and Class Members' payments because Defendants failed to adequately protect their PHI.

187. Plaintiff and Class members have no adequate remedy at law.

188. As a direct and proximate result of the Data Breach which Defendants permitted to occur, Plaintiff and the Class have suffered or will imminently suffer actual, tangible, injury-in-fact and damages, including, without limitation: monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress; fraudulent misuse of PHI to attempt to obtain credit and loans; loss of the opportunity to control how their PHI is used; diminution in value of their PHI; compromise and continuing publication of their PHI; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; other unauthorized use of stolen PHI; the continued risk to their PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PHI in their possession.

189. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because

of their misconduct and Data Breach.

COUNT VI
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

190. Plaintiff realleges and reincorporates the preceding paragraphs as if fully set forth herein.

191. Plaintiff and the Class Members had a legitimate expectation of privacy to their PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

192. Defendants owed a duty to Plaintiff and the Class Members to keep their PHI confidential.

193. Defendants failed to protect Plaintiff's and the Class's PHI and failed to ensure that its vendors protected said PHI and exposed the PHI of Plaintiff and the Class Members to unauthorized persons in the Data Breach.

194. In the Data Breach, Defendants allowed unauthorized third parties access to and examination of the PHI of Plaintiff and the Class Members, by way of Defendants' failures to protect the PHI and ensure that vendors protected that PHI.

195. The unauthorized release to, custody of, and examination by unauthorized third parties of the PHI of Plaintiff and the Class Members is highly offensive to a reasonable person.

196. The intrusion was into a place which a reasonable person would consider private and which is entitled to be private. Plaintiff's and the Class Members' PHI was disclosed to Defendants in connection with receiving medical or other services, but privately with an intention that the PHI would be kept confidential and would be protected from unauthorized disclosure.

197. Plaintiff and the Class Members were reasonable in their belief that such

information would be kept private and would not be disclosed without their authorization.

198. The Data Breach constitutes an intentional or reckless interference by Defendants with Plaintiff's and the Class Members' privacy, of a kind that would be highly offensive to a reasonable person.

199. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they had actual knowledge that their data security practices, including the supervision of its vendors' data security practices, were inadequate and insufficient.

200. Defendants acted with reckless disregard for Plaintiff's and Class Members' privacy when they allowed improper access to its systems containing Plaintiff's and Class Members' PHI, or when it transmitted Plaintiff's and Class Members' PHI to a vendor without ensuring the vendor utilized adequate data security measures to protect that PHI.

201. Defendants was aware of the potential of a data breach and failed to adequately safeguard their systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PHI, and/or failed to ensure that its vendor adequately safeguarded its systems and implemented appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PHI.

202. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

203. As a direct and proximate result of Defendants' invasion of privacy, Plaintiff and the Class have suffered or will imminently suffer actual, tangible, injury-in-fact and damages, including, without limitation: monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress; fraudulent misuse of PHI to

attempt to obtain credit and loans; loss of the opportunity to control how their PHI is used; diminution in value of their PHI; compromise and continuing publication of their PHI; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; other unauthorized use of stolen PHI; the continued risk to their PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PHI in their possession.

204. As a result, Plaintiff and the Class Members are entitled to recover actual and compensatory damages in an amount to be proven at trial, and punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, REGINALD SMITH, individually, and on behalf of all others similarly situated, demands judgment against Defendants and request that the Court enter an order as follows:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable actual, compensatory, exemplary, and punitive damages, as allowed by law;

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

D. Awarding declaratory and other equitable relief as is necessary to protect the

interests of Plaintiff and the Class;

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

F. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PHI;

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

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

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

J. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff, pursuant to Fed. R. Civ. P. 38, demands a trial by jury on all issues so triable.

Dated: August 12, 2024

Respectfully submitted,

/s/Samuel J. Strauss
Samuel J. Strauss (WI Bar #1113942)
Raina C. Borrelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI, PLLC
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
sam@straussborrelli.com
raina@straussborrelli.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801

(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Counsel for Plaintiff and the Proposed Class

ClassAction.org
