

**STATE OF MICHIGAN
7th JUDICIAL CIRCUIT
GENESEE COUNTY**

Cindy Womack-Devereaux, Sue Ranney, Kayle Gries, Cheryl Drugich, Janise Norwood, Melissa Porter, Jamie McSkulin, Tamyra Ejuan Wells, Ashley Beasley, Kyle Turri, and Janie Montgomery individually and on behalf of those similarly situated,

Plaintiffs,

v.

McLaren Health Care Corporation,

Defendant.

Case No. 24-121459
Hon. B. Chris Christenson

**CLASS ACTION
JURY TRIAL DEMANDED**

**AMENDED CONSOLIDATED CLASS
ACTION COMPLAINT**

E. Powell Miller (P39487)
Emily E. Hughes (P68724)
THE MILLER LAW FIRM
950 W. University Drive, Suite 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com

Gary M. Klinger*
MILBERG, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
T: (866) 252-0878
gklinger@milberg.com

Benjamin F. Johns
Samantha E. Holbrook
SHUB JOHNS & HOLBROOK LLP
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
T: (610) 477-8380
bjohns@shublawyers.com
sholbrook@shublawyers.com

Interim Co-Lead Counsel

Timothy J. Lowe (P68669)
MCDONALD HOPKINS LLC
39533 Woodward Ave., Ste. 318
Bloomfield Hills, MI 48304
T: (248) 220-1359
tlowe@mcdonaldhopkins.com

Christopher G. Dean (*pro hac vice*)
MCDONALD HOPKINS LLC
600 Superior Avenue, East, Suite
2100 Cleveland, Ohio 44114
T: (216) 348-5400
cdean@mcdonaldhopkins.com

J. Brian MacDonald (P25887)
R. Paul Vance (P68894)
CLINE, CLINE & GRIFFIN, P.C.
503 South Saginaw St., Ste. 1000
Flint, MI 48502
(810) 232-3141
bmacdonald@ccglawyers.com
pvance@ccglawyers.com

Counsel for Defendant

Samuel J. Strauss*
Raina Borelli (*pro hac vice*)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
(872) 263-1100
sam@straussborrelli.com
raina@straussborrelli.com

Additional Plaintiffs' Counsel

**Pro Hac Vice Application Forthcoming*

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Cindy Womack-Devereaux, Sue Ranney, Kayle Gries, Cheryl Drugich, Janise Norwood, Melissa Porter, Jamie McSkulin, Tamyra Ejuan Wells, Ashley Beasley, Kyle Turri, and Janie Montgomery (collectively, “Plaintiffs”) bring this Amended Master Consolidated Class Action Complaint against McLaren Health Care Corporation (“McLaren” or “Defendant”), individually and on behalf of all others similarly situated, and allege upon personal knowledge as to themselves and information and belief as to all other matters as follows:

NATURE OF THE ACTION

1. Healthcare providers that are entrusted with patients’ sensitive personally identifying information (“PII”) or protected health information (“PHI”) (together, “Private Information”) owe a duty of care to those individuals to protect that information. This duty arises because it is foreseeable that the exposure of PII and PHI to unauthorized persons – especially hackers and other cybercriminals with nefarious intentions – will result in harm to the affected individuals.

2. Because of the highly sensitive nature of the data collected and maintained during the course of providing patient care, healthcare providers like McLaren are leading targets for

cyber-attacks. The rapid growth of electronic medical recordkeeping, online medical services, and mobile medical apps has created new pressure points for criminals to exploit.

3. States have enacted strict laws requiring entities that collect and maintain patient information to ensure they take the utmost care to protect the privacy of the data they hold. In 2004, for example, Michigan enacted the Identify Theft Protection Act (MCL 445.61, *et seq.*), requiring entities that have experienced a data breach to promptly notify those affected of the nature and quality of the breach.

4. McLaren itself recognizes the importance of data security, telling patients that “[w]e protect the privacy of your health information” and “we seek to use reasonable measures to protect Personally Identifiable Information[.]”¹

5. Despite this professed recognition, McLaren failed to take appropriate measures to safeguard the sensitive data entrusted to it from the foreseeable event of a data breach.

6. According to McLaren, “there was unauthorized access to McLaren’s network between July 28, 2023 and August 23, 2023”² (herein after the “2023 Data Breach”). For nearly a month, unauthorized hackers were able to access the McLaren computer network and extract 3.2 TB of data without being detected.

7. McLaren claims to have first become aware of “suspicious activity related to its computer systems” on August 22, 2023. But it was not until October 20, 2023 that it began to provide “substitute . . . website and media notice,” and then not until November 9, 2023 that it began mailing notification of the Data Breach directly to its current and former patients and other

¹ <https://www.mclaren.org/main/web-privacy-policy> (last accessed August 8, 2024).

² <https://apps.web.maine.gov/online/aeviewer/ME/40/40c59f93-d7fd-4133-8148-a05a244b96b7.shtml> (last accessed August 30, 2024).

affiliated persons.³

8. According to McLaren’s notice, it determined that “the unauthorized actor had the ability to acquire certain information stored on the network during the period of access” and that “information pertaining to certain individuals may have been included in the potentially accessed files” – the compromised data included names, Social Security numbers, health insurance information, birthdates, and medical information (including diagnosis, physician information, “prescription/ medication information,” and “diagnostic and treatment information.”)⁴

9. Upon information and belief, McLaren’s form letters to its current and former patients and other affiliated persons did not identify who the “unauthorized actor” was, address whether a ransomware demand was made and/or paid, or indicate if any of the compromised patient data had been placed on the dark web (the illicit marketplace where thieves and criminals trade stolen PII and PHI in bulk).

10. A report issued on October 4, 2023, revealed that the notorious hacking collective BlackCat/AlphV had posted “that it stole 6 terabytes of McLaren’s data” and further boasted about this being “one of the biggest leaks of all time” – the group is claimed to have told McLaren “[o]ur backdoor is still running on your network.”⁵

11. On October 6, 2023, Michigan Attorney General Dana Nessel issued a press release which indicated that that “[c]ybercriminal gang ALPHV (or BlackCat) has claimed responsibility for the theft of the sensitive personal health information (PHI) of 2.5 million McLaren patients.”⁶ The press release stated that this cybercriminal group had also been linked to the recent attack at

³ *Id.*

⁴ *Id.*

⁵ *Id.*

⁶ <https://www.michigan.gov/ag/news/press-releases/2023/10/06/ag-nessel-notifies-michigan-residents-of-mclaren-ransomware-attack> (last accessed August 30, 2024).

MGM Resorts, and had posted a message on the dark web the previous week claiming that “the McLaren data was on the dark web and would be released in a few days unless a ransomware payment was received.”⁷

12. Attorney General Nessel stated in this press release that “[o]rganizations that handle our most personal data have a responsibility to implement safety measures that can withstand cyber-attacks and ensure that a patient’s private health information remains private” – and she also indicated “[t]ime is of the essence when a breach occurs to ensure affected individuals can take the necessary steps to protect their identities.”⁸

13. Despite having experienced the 2023 Data Breach less than a year ago, McLaren failed to make the necessary security upgrades to ensure the protection of its systems and of the Private Information of Plaintiffs and the Class going forward.

14. Accordingly, due to these failures, McLaren experienced *another* data security incident nearly a year later. Pursuant to a statement issued by McLaren on August 7, 2024, “McLaren Health Care can now confirm the disruption to our information technology and phone systems that was reported yesterday [August 6, 2024] was the result of a criminal cyber attack.”⁹

15. Upon information and belief, McLaren first became aware of this external breach even earlier (hereinafter known as “2024 Data Breach”), on August 5, 2024, through a ransomware demand sent through and among its information technology systems.¹⁰

16. As a result of McLaren’s inadequate security measures, and in breach of its legal

⁷ *Id.*

⁸ *Id.*

⁹ <https://www.mclaren.org/main/notification> (last accessed August 8, 2024).

¹⁰ <https://www.lansingstatejournal.com/story/news/local/2024/08/17/ransomware-attack-mclaren-health-care-patients-services-appointments/74840781007/> (last accessed September 11, 2024).

duties and obligations, both the 2023 Data Breach and the 2024 Data Breach (collectively, “Data Breaches”) occurred, putting the Private Information of Plaintiffs and the Class at risk for the foreseeable future.

17. As a result of the Data Breaches, Plaintiffs and the putative Class suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (vii) loss of employment opportunities; and (viii) the continued and certainly increased risk to their Private Information, which upon information and belief: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

18. Plaintiffs’ claims are brought as a class action, pursuant to MCR 3.501, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of a similarly situated class of individuals for negligence, breach of implied contract, breach of express contract, violations of the Michigan Consumer Protection Act, violations of the Michigan Data Breach Notification Statute, and, alternatively, unjust enrichment. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

19. Plaintiffs seek remedies including, but not limited to, compensatory, nominal, punitive and statutory damages, as well as injunctive relief mandating improvements to McLaren’s

data security systems and the provision of appropriate identity theft and monitoring services.

PARTIES

20. Plaintiff Cindy Womack-Devereaux is a natural born person and citizen of Michigan, where she intends to remain. Plaintiff Womack-Devereaux is a McLaren Health patient.

21. Plaintiff Sue Ranney is a natural person and citizen of Michigan, where she intends to remain. Plaintiff Ranney is a McLaren Health patient.

22. Plaintiff Kayle Gries is a natural person and citizen of Hubbard Lake, Michigan, where she intends to remain. Plaintiff Gries is a McLaren Health patient and employee.

23. Plaintiff Cheryl Drugich is a natural person and citizen of Michigan, where she intends to remain. Plaintiff Drugich is a current patient at McLaren.

24. Plaintiff Janise Norwood is a natural person and citizen of Michigan, where she intends to remain. Plaintiff Norwood is a current patient at McLaren.

25. Plaintiff Melissa Porter is a natural person and citizen of Michigan, where she intends to remain. Plaintiff Porter is a current patient at McLaren.

26. Plaintiff Jamie K. McSkulin is a natural person and citizen of Michigan, where she intends to remain. Plaintiff McSkulin is a current patient at McLaren.

27. Plaintiff Tamyra Ejuan Wells is a natural person and citizen of Michigan, where she intends to remain. Plaintiff Wells is a current patient at McLaren.

28. Plaintiff Ashley Beasley is a natural person and citizen of Michigan, where she intends to remain. Plaintiff Beasley is a former patient at McLaren.

29. Plaintiff Kyle Turri is a natural person and citizen of Michigan, where he intends to remain. Plaintiff Turri is a former patient at McLaren.

30. Plaintiff Janie Montgomery is a natural person and citizen of Pontiac, Michigan, where she intends to remain. Plaintiff Montgomery is a patient at McLaren.

31. Defendant McLaren Health Care Corporation is a non-profit corporation organized under the state laws of Michigan. Its principal place of business is in Grand Blanc, Michigan, in the County of Genesee.

JURISDICTION AND VENUE

32. This Court has subject matter jurisdiction over this action pursuant to MCL 600.605.

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

34. Venue is proper in this Court under MCL 600.1629(1)(a)(i) because Defendant's principal place of business is in this county and the acts and omissions giving rise to Plaintiffs' claims emanated from this county.

FACTUAL ALLEGATIONS

Background

35. McLaren "is a \$6.6 billion, fully integrated health care delivery system" that "includes 13 hospitals in Michigan, ambulatory surgery centers, imaging centers, a 490-member employed primary and specialty care physician network, commercial and Medicaid HMOs covering more than 732,838 lives in Michigan and Indiana[.]"¹¹

36. Members of the proposed class here, which includes Plaintiffs, are current and former employees, contractors, and patients of McLaren and other affiliated persons whose PII

¹¹ <https://www.mclaren.org/main/about-mclaren-health-care> (last accessed August 8, 2024).

and/or PHI was compromised as a result of the Data Breaches (“Class Members”).

37. McLaren creates, collects, and receives treatment records, lab testing data, demographic information, and payment information from its employees, contractors, patients, and other affiliated persons. Employees, contractors, and patients entrusted McLaren with this information, which, by its nature, is confidential and highly sensitive and may include their Social Security numbers, medical histories, current conditions, medications, credit card numbers, and other sensitive PII and PHI.

38. Because of the highly sensitive nature of the information it collects, McLaren makes many promises regarding the protection of patient data. Its Compliance Program and Resources page, for example, contains a “pledge” to protect the privacy of patient’s data:

Our Pledge to You

McLaren Health Care understands that health information about you is private and personal, and we are committed to protecting it. We protect the privacy of your health information because it is the right thing to do. We follow federal and state laws that govern your health information. Each time you visit a hospital, physician or other health care provider, a record of your visit is made. Our Privacy Notice and The Health Insurance Portability and Accountability Act of 1996 (HIPAA) responsibilities apply to the records of your care at McLaren, whether created by facility staff or your personal physician. We are required by law to make sure that health information that identifies you is kept private, to provide you with access to our Notice of Privacy Practices outlining our legal duties concerning your health information, and to follow the terms of the Privacy Notice that is currently in effect.

McLaren’s 2020 Standards of Conduct claims:

A COMMITMENT TO CONFIDENTIALITY AND ELECTRONIC SECURITY [. . .]

It is the responsibility of every employee, physician, volunteer, and contractor or vendor to adhere to regulations, policies/procedures, and patient rights for privacy . . .

39. McLaren’s June 2022 Notice of Privacy Practices claims:

OUR PLEDGE TO YOU

We understand that health information about you is private and personal, and we are

committed to protecting it. [. . .]

Notification of a Breach: If our actions result in a breach of your unsecured health information we will notify you of that breach.

40. Indeed, the Privacy Policy posted on Defendant’s website provides that: “we seek to use reasonable measures to protect Personally Identifiable Information[.]”¹²

41. Plaintiffs and Class Members, as former and current employees, contractors, and patients of McLaren and other affiliated persons, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when PHI and other sensitive PII is involved.

42. McLaren did not keep its pledge to maintain patient, employee, and contractor privacy. Based on the nature of the PII and PHI, upon information and belief, the ransom demanded by the unauthorized users who gained access to the McLaren networks, it is apparent that McLaren’s system failed to employ reasonable and appropriate security measures with regard to any or all of the following: storing data in secure, offline locations; encrypting private records and data; using up-to-date software equipped with standard security patches; using anti-virus applications that block malicious code from external sources; and implementing policies requiring all workers with system access to use https protocols when using online tools.

43. Defendant’s failure to adequately employ these and other industry-standard security measures needlessly exposes employees, contractors, patients, and other affiliated persons whose data was stored with Defendant to the risk of data theft.

¹² <https://www.mclaren.org/main/web-privacy-policy> (last accessed August 8, 2024).

The 2023 Data Breach

44. On or around August 22, 2023, McLaren “detected ‘suspicious activity’ on its computer network, immediately launched an investigation into the source of the disruption, and retained outside global cybersecurity specialists to assist[.]”¹³

45. As a result of its investigation, Defendant “determined that [McLaren] did experience a ransomware event.”¹⁴

46. On or about September 29, 2023, ALPHV ransomware cybercrime collective, also known as BlackCat, took credit for the ransomware attack and further claimed “to have stolen 6 terabytes of data on 2.5 million patients[.]”¹⁵

47. BlackCat was a threat actor known to Defendant at the time the 2023 Data Breach occurred and Defendant had been warned of its methods and strategies. In January 2023, the US Department of Health and Human Services’ Office of Information Security and Health Sector Cybersecurity Coordination Center issued a joint statement and brief warning entities in the healthcare sector, including McLaren, that ransomware attacks from BlackCat posed a specific threat to the industry.¹⁶ The warning specified the operating systems that were especially vulnerable to attack, entry points it was likely to use to access data, the technical operations it employed to attack targets, the tools it used to access and exfiltrate data, and a series of mitigation and defense strategies healthcare providers should use to defend their patients’ PHI and PII.¹⁷

48. Based on the nature of the 2023 Data Breach and the statements of the unauthorized

¹³ <https://www.databreachtoday.com/group-claims-stole-25-million-patients-data-in-attack-a-23212> (last accessed August 30, 2024).

¹⁴ *Id.*

¹⁵ *Id.*

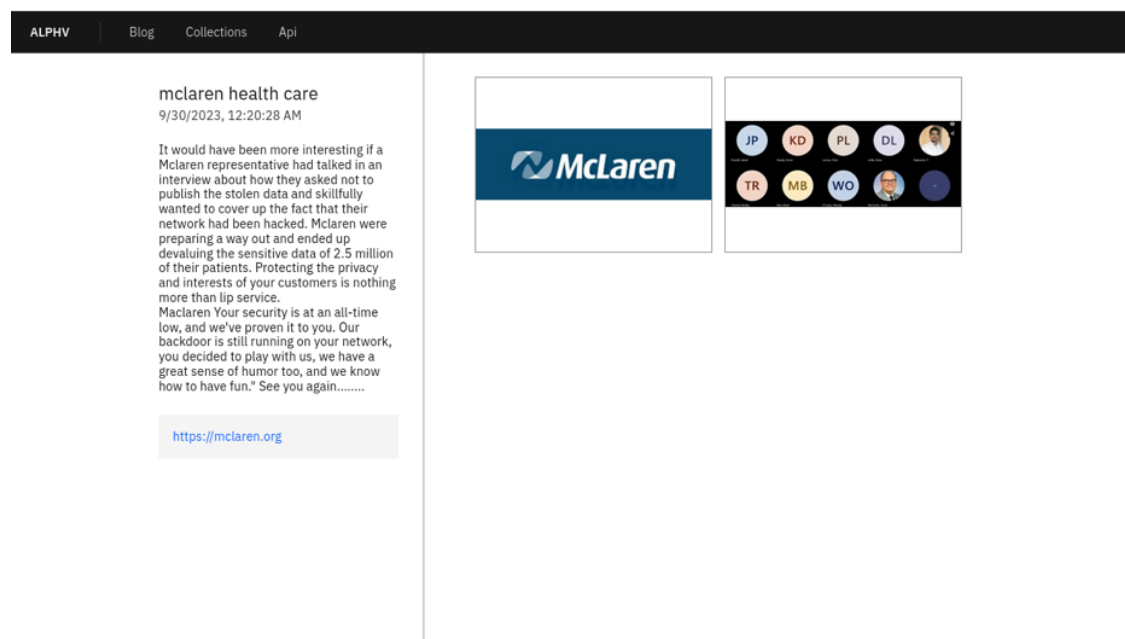
¹⁶ <https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf> (last accessed August 30, 2024).

¹⁷ *Id.*

users who gained access to the McLaren networks, Plaintiffs allege, on information and belief, that Defendant failed or refused to heed the warnings from the January 2023 briefing, continued to use vulnerable systems, and neglected to employ the mitigation and defense strategies it was urged to use, which resulted in the 2023 Data Breach.

49. Upon information and belief, Blackcat attempted to negotiate a ransom with Defendant.

50. When BlackCat announced the 2023 Data Breach publicly on its TOR leak site on September 30, 2023, it indicated that it still had access to the McLaren network through backdoors that remained open.



51. The message published by BlackCat on its leak site reads: “It would have been more interesting if a McLaren [sic] representative had talked in an interview about how they asked not to publish the stolen data and skillfully wanted to cover up the fact that their network had been hacked. McLaren were preparing [sic] a way out and ended up devaluing the sensitive data of 2.5 million of their patients. Protecting the privacy and interests of your customers is nothing more

than lip service. McLaren [sic] Your security is at an all-time low, and we've provien [sic] it to you. Our backdoor is still running on your network, you decided to play with us, we have a great sense of humor too, and we know how to have fun.' See you again[.]”

52. Follow up posts on the BlackCat TOR leak site provide evidence of the data exfiltrated from McLaren including database scheme (including table names), screen shots of table rows with fields and data, and directory structures.

53. BlackCat then posted on its TOR leak site on October 4, 2023 that it had confirmed to McLaren the data in its possession and would start auctioning data within 72 hours, with time remaining to salvage McLaren's data security reputation, inferring that there was still time to pay an unpaid ransom. Notably, McLaren did not disclose this fact in its Notice Letter, nor did it alert Plaintiffs and Class Members that BlackCat had acquired over 6 terabytes of McLaren's data.

54. Then, on October 19, 2023, a threat actor, “IAmNietzsche,” started selling McLaren data on the forum_XSS for \$50,000. On the post, IAmNietzsche provided screenshots of the McLaren data, which showed details such as patient information, insurance details, lab test data, doctor information, visit information, and medication management system data. The total size of the database was approximately 3.2 TB.

55. The data remained for sale on the dark web through at least the following month. By November 7, 2023, IAmNietzsche was still selling the data at the reduced price of \$15,000.

56. While it is not known with certainty how BlackCat gained access to McLaren's network, it is clear that there were thousands of McLaren credentials readily available on the dark web. The availability of those credentials suggests a canary in the coal mine warning of inadequate security practices in the overall culture at McLaren.

57. In the period between July 28, 2023 and August 22, 2023, BlackCat and/or its

affiliate, had removed 3.2 TB of data from the McLaren network undetected. This suggests there is a lack of security controls and policies in place that should have detected and prevented this type of incident from occurring.

58. A ransomware attack is a type of cyberattack that is frequently used to target companies due to the sensitive patient data they maintain.¹⁸ In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.¹⁹

59. Ransomware attackers do not just hold networks hostage: “ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue.”²⁰ As cybersecurity expert Emsisoft warns, “[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence [...] the initial assumption should be that data may have been exfiltrated.”

60. An increasingly prevalent form of ransomware attack is the “encryption+exfiltration” attack in which the attacker encrypts a network and exfiltrates the data contained within.²¹ In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.²² Once the data is exfiltrated from a network, its confidential nature is

¹⁸ *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at <https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/> (last accessed August 30, 2024).

¹⁹ *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at <https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends> (last accessed August 30, 2024).

²⁰ *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at <https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/> (last accessed August 30, 2024).

²¹ *2020 Ransomware Marketplace Report*, available at <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report> (last accessed August 30, 2024).

²² *Ransomware FAQs*, available at <https://www.cisa.gov/stopransomware/ransomware-faqs> (last accessed August 30, 2024).

destroyed and it should be “assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt” – and even where companies pay for the return of data, attackers often leak or sell the data regardless because there is no way to verify that copies of the data are destroyed.²³

61. Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates.²⁴ In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.²⁵

62. Upon information and belief, the cyberattack here was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains Private Information on its computer networks and/or systems.

63. Plaintiffs’ and Class Members’ Private Information was compromised and acquired in the 2023 Data Breach.

64. The files containing Plaintiffs’ and Class Members’ Private Information that were targeted and stolen from Defendant included Plaintiffs’ and Class Members’ PII and/or PHI.

65. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiffs and Class Members.

66. As evidenced by the 2023 Data Breach’s occurrence, the Private Information

²³ *Id.*

²⁴ *Ponemon study finds link between ransomware, increased mortality rate*, available at <https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate> (last accessed August 30, 2024).

²⁵ *The State of Ransomware in Healthcare 2022*, available at <https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf> (last accessed August 30, 2024).

contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

The 2024 Data Breach

67. Upon information and belief, the 2024 Data Breach occurred on or around August 5, 2024.

68. According to a statement issued by McLaren on August 7, 2024, "McLaren Health Care can now confirm the disruption to our information technology and phone systems that was reported yesterday [August 6, 2024] was the result of a criminal cyber attack."²⁶

69. Upon information and belief, McLaren first became aware of this breach on August 5, 2024, through a ransomware demand sent through and among its information technology systems.

70. According to McLaren's August 7, 2024 statement, its "information technology team continues to work with external cyber security experts to analyze the nature of the attack and mitigate the impacts of the threat actors."²⁷

71. Upon information and belief, the unauthorized users who gained access to McLaren's networks advised McLaren that they had stolen Private Information and would release the data unless a ransom was paid through the dark web.

72. Based on the nature of the 2024 Data Breach and the statements of the unauthorized users who gained access to the McLaren networks, Plaintiffs allege, on information and belief, that Defendant failed or refused to heed the warnings from McLaren's 2023 Data Breach, continued to use vulnerable systems, and neglected to employ the mitigation and defense strategies it was urged

²⁶ <https://www.mclaren.org/main/notification> (last accessed August 8, 2024).

²⁷ *Id.*

to use, which resulted in the 2024 Data Breach.

73. Especially given the proximity of the most recent data breach at McLaren, this suggests that there is a lack of security controls and policies in place that should have detected and prevented this type of incident from occurring.

74. As evidenced by the 2024 Data Breach's occurrence, upon information and belief, the Private Information contained in Defendant's network was not encrypted.

75. Defendant had obligations created by the FTC Act, HIPAA, contract, state and federal law, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

Data Breaches Are Preventable

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

77. McLaren could have prevented the Data Breaches by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Private Information.

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

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

Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/ LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.²⁸

²⁸ *Ransomware FAQs*, available at <https://www.cisa.gov/stopransomware/ransomware-faqs> (last accessed August 8, 2024).

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

Secure internet-facing assets

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

Thoroughly investigate and remediate alerts

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

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].²⁹

80. Given that Defendant was storing the Private Information of its current and former patients, employees, contractors, and other affiliated persons, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

81. The occurrence of the Data Breaches indicates that Defendant failed to adequately

²⁹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last accessed August 8, 2024).

implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breaches and the exposure of the Private Information, including that of Plaintiffs and Class Members.³⁰

Defendant Acquires, Collects, and Stores Patients' Private Information

82. Defendant acquires, collects, and stores a massive amount of Private Information on its current and former patients, employees, contractors, and other affiliated persons.

83. As a condition of obtaining medical services or employment at McLaren, Defendant requires that patients, employees, and contractors entrust it with highly sensitive Private Information.

84. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information, McLaren assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

85. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

86. Plaintiffs and Class Members relied on McLaren to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and make only authorized disclosures of this information.

McLaren Knew That Cybercriminals Target Private Information

87. McLaren's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect

³⁰ <https://www.databreachtoday.com/group-claims-stole-25-million-patients-data-in-attack-a-23212> (last accessed August 8, 2024).

and store Private Information, like Defendant, preceding the dates of the Data Breaches. McLaren knew that the sensitive personal data with which it was entrusted would be a lucrative target for hackers.

88. This is even more notable given the fact that McLaren experienced two data breaches within the span of one year, and was on notice after the 2023 Data Breach that another breach was likely to occur if it did not improve its systems.

89. Despite such knowledge, McLaren failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyber-attacks that McLaren should have anticipated and guarded against.

90. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

91. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.³¹

92. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), and Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

93. Cybercriminals seek out PHI at a greater rate than other sources of personal

³¹ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/> (last accessed August 8, 2024).

information. In a 2023 report, the healthcare compliance company Protenu found there were 956 medical data breaches in 2022 with over 59 million patient records exposed. This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenu compiled in 2020.

94. Defendant knew and understood that unprotected or exposed Private Information in the custody of healthcare entities, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

95. At all relevant times, McLaren knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

96. Indeed, cyber-attacks, such as the ones experienced by McLaren, have become so notorious that the Federal Bureau of Investigation and US Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."³²

97. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class Members are incurring and

³² https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed August 8, 2024).

will continue to incur such damages in addition to any fraudulent use of their Private Information.

98. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

99. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

100. As a healthcare entity in custody of the Private Information of current and former patients, employees, contractors, and other affiliated persons, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

101. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."³³ The FTC describes "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."³⁴

³³ 17 CFR 248.201 (2013).

³⁴ *Id.*

102. PII and PHI are valuable property rights. Their value as a commodity is measurable. “Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks.”³⁵ American companies are estimated to have spent over \$19 billion on acquiring personal data of consumers in 2018. It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the cyber black market or the dark web, for many years.

103. The PHI/PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.³⁶

104. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, Private Information, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated, becoming more valuable to thieves and more damaging to victims.

105. For example, PII can be sold at a price ranging from \$40 to \$200.³⁷ Bad actors can

³⁵ *Exploring the Economics of Personal Data*, available at: https://www.oecd-ilibrary.org/exploring-the-economics-of-personal-data_5k486qtxldmq.pdf (last accessed August 8, 2024).

³⁶ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed August 8, 2024).

³⁷ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web> (last accessed August 8, 2024).

purchase access to entire company data breaches from \$900 to \$4,500.³⁸

106. PII can sell for as much as \$363 per record according to the Infosec Institute.³⁹ PII is particularly valuable because criminals can use it to target victims with frauds and scams.

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

108. PHI is particularly valuable and has been referred to as a “treasure trove for criminals” – a cybercriminal who steals a person’s PHI can end up with as many as “seven to ten personal identifying characteristics of an individual.”⁴⁰

109. Theft of PHI is also 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.”⁴¹

110. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.⁴²

111. Based on the foregoing, the information compromised in the Data Breaches is significantly more valuable than the loss of, for example, payment card information in a retailer

³⁸ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed August 8, 2024).

³⁹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last accessed August 8, 2024).

⁴⁰ *What Happens to Stolen Healthcare Data?*, available at: <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (last accessed August 8, 2024).

⁴¹ See <https://efraudprevention.net/home/education/?a=187> (last accessed August 8, 2024).

⁴² Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (October 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed August 8, 2024).

data breach because, there, victims can cancel or close credit and debit card accounts. Upon information and belief, the information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

112. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”⁴³

113. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

114. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. 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.⁴⁴

McLaren Fails to Comply With FTC Guidelines

115. The 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.

⁴³ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed August 8, 2024).

⁴⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed August 8, 2024).

116. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These 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 problems.⁴⁵

117. The guidelines also recommend that healthcare 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.⁴⁶

118. The FTC further recommends that healthcare companies not maintain Private 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.

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

⁴⁵ *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 accessed August 8, 2024).

⁴⁶ *Id.*

their data security obligations.

120. 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 (McLaren) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

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

122. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to patients’ Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 USC 45.

123. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients, employees, contractors, and other affiliated persons, and it was also aware of the significant repercussions that would result from its failure to do so.

McLaren Fails to Comply With HIPAA Guidelines

124. Defendant is a covered entity under HIPAA (45 CFR 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 CFR Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 CFR Part 160 and Part 164, Subparts A and C.

125. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).⁴⁷ See

⁴⁷ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected

42 USC 17921, 45 CFR 160.103.

126. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

127. HIPAA’s Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred electronically.

128. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 CFR 164.302.

129. “Electronic protected health information” is “individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media.” 45 CFR 160.103.

130. HIPAA’s Security Rule requires Defendant to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

131. HIPAA also requires Defendant to “review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 CFR 164.306(e). Defendant is also required under

health information. HITECH references and incorporates HIPAA.

HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 CFR § 164.312(a)(1).

132. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. See 45 CFR § 164.306(a)(1) and § 164.306(a)(3); see also 42 USC §17902.

133. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and in no case later than 60 days following discovery of the breach.”⁴⁸

134. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 CFR Part 164, Subparts D or E. See 45 CFR § 164.530(e).

135. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 CFR Part 164, Subpart E by the covered entity or its business associate. See 45 CFR § 164.530(f).

136. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 CFR §§ 164.302-164.318. For example, “HHS has developed

⁴⁸ Breach Notification Rule, US Dep’t of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added) (last accessed August 8, 2024).

guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.”⁴⁹ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.”⁵⁰

McLaren Fails to Comply With Industry Standards

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

138. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

139. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network

⁴⁹ US Department of Health & Human Services, Security Rule Guidance Material, <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> (last accessed August 8, 2024).

⁵⁰ US Department of Health & Human Services, Guidance on Risk Analysis, <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last accessed August 8, 2024).

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. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

140. On information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), which are all established standards in reasonable cybersecurity readiness.

141. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendant 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.

Common Injuries and Damages

142. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.

143. As a result of Defendant's ineffective and inadequate data security practices and the resulting Data Breaches, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred

mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; (f) loss of employment opportunities; and (g) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

The Data Breaches Increase Victims' Risk of Identity Theft

144. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Experian, one of the largest credit reporting companies in the world, warns consumers that identity thieves can profit off their personal information by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.

145. Upon information and belief, an unauthorized threat actor is in possession of the Private Information and intends to release the Private Information for sale on the dark web, if it has not already done so. Unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

146. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other

criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

147. Because a person's identity is akin to a puzzle with multiple data points, 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 track the victim to attempt other crimes against the individual to obtain more data to perfect a crime.

148. 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. A data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

149. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.⁵¹

⁵¹ “Fullz” describes data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (September 18, 2014), available at <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm> (last accessed August 8, 2024).

150. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information 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.

151. The development of “Fullz” packages means that the stolen Private Information from the Data Breaches here can easily be used to link and identify it to Plaintiffs’ and Class Members’ 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 Private Information that was exfiltrated in the Data Breaches, criminals may still 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.

152. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the Data Breaches can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and Class Members.

153. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their Social Security number, and a new Social Security number will not be provided until after the harm has already been suffered by the victim.

154. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other Private Information (e.g., names, addresses, and dates of birth) is akin to having a master key to the gates of fraudulent activity. Data security researcher Tom Stickley, hired by companies to find flaws in their computer systems, has stated, “If I have

your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings.”⁵² Then, this comprehensive dossier can be sold—and then resold in perpetuity—to bad actors (i.e., scam telemarketers).

155. Theft of Private Information is even more serious when it includes theft of PHI. Data breaches involving medical information “typically leave[] a trail of falsified information in medical records that can plague victims’ medical and financial lives for years.”⁵³ It “is also more difficult to detect, taking almost twice as long as normal identity theft.”⁵⁴ In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Private Information “to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care.”⁵⁵ The FTC also warns, “If the thief’s health information is mixed with yours it could affect the medical care you’re able to get or the health insurance benefits you’re able to use.”⁵⁶

156. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services neither sought nor received.

⁵² Patrick Lucas Austin, *‘It Is Absurd.’ Data Breaches Show it’s Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), <https://time.com/5643643/capital-one-equifax-data-breach-social-security> (last accessed August 8, 2024).

⁵³ *Medical Identity Theft*, available at: <https://www.worldprivacyforum.org/category/med-id-theft> (last accessed August 8, 2024).

⁵⁴ *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, available at: <https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf> (last accessed, August 8, 2024).

⁵⁵ *What To Know About Medical Identity Theft*, available at: <https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last accessed August 8, 2024).

⁵⁶ *Id.*

- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime. For example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed due to medical activities of the imposter; and victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.⁵⁷

157. There may also be a time lag between when sensitive personal information is stolen, when it is illicitly used, and when a person discovers the illicit usage. For example, it takes approximately three months on average for consumers to discover that their identity has been stolen and used, but it takes some individuals up to three years to learn that information.

158. It is within this context that Plaintiffs and Class Members must now live with the knowledge that, upon information and belief, their Private Information is forever in cyberspace and was taken by and in the possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

⁵⁷ *The Geography of Medical Identity Theft*, available at: https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf (last accessed August 8, 2024).

Loss of Time to Mitigate Risk of Identity Theft and Fraud

159. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified that their Private Information has been compromised, as in the Data Breaches, a reasonable person is expected to take steps and time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose an individual to greater financial harm – ultimately, the resource and asset of time has been lost.

160. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

161. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as monitoring their accounts for fraudulent activity and checking their credit reports for unusual activity.

162. Plaintiffs’ and Class Members’ mitigation efforts, including those who experience actual identity theft and fraud, are consistent with the US Government Accountability Office’s 2007 report regarding data breaches, the 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.”⁵⁸

163. Plaintiffs’ mitigation efforts are also consistent with the steps that the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (if someone steals

⁵⁸ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), available at: <https://www.gao.gov/new.items/d07737.pdf> (last accessed August 8, 2024).

their identity, an extended fraud alert that lasts for seven years is suggested), 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.⁵⁹

Diminution of Value of Private Information

164. PII and PHI are valuable property rights.⁶⁰ Their value is axiomatic, considering the value of an individual's data in today's economy and 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.

165. A robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁶¹

166. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{62,63}

167. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁶⁴

168. As a result of the Data Breaches, Plaintiff' and Class Members' Private Information,

⁵⁹ See Federal Trade Commission, *Identity Theft.gov*, available at: <https://www.identitytheft.gov/Steps> (last accessed August 8, 2024).

⁶⁰ See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich JL & Tech 11, at *3-4 (2009) ("Private Information, 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).

⁶¹ See <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last accessed August 8, 2024).

⁶² <https://datacoup.com/> (last accessed August 8, 2024).

⁶³ <https://digi.me/what-is-digime/> (last accessed August 8, 2024).

⁶⁴ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last accessed August 8, 2024).

which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

169. Thus, the information compromised in the Data Breaches is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Upon information and belief, the information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

170. Among other forms of fraud, identity thieves may obtain driver’s licenses, which can then lead to improper procurement of government benefits, medical services, and housing, and even giving false information to police.

171. The fraudulent activity resulting from the Data Breaches may not come to light for years.

172. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

173. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s network, amounting to the detailed Private Information of, upon information and belief, millions of individuals, and thus, the significant number of

individuals who would be harmed by the exposure of the unencrypted data.

174. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

175. Given the type of targeted attack in this case and related sophisticated criminal activity, upon information and belief, the type of Private Information involved and the volume of data obtained in the Data Breaches, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes (e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims).

176. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her personal information 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.

177. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

178. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from Defendant's Data Breaches.

Loss of the Benefit of the Bargain

179. Furthermore, McLaren's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to employment at Defendant or agreeing to pay Defendant and/or its agents for the provision of medical services, directly or indirectly, Plaintiffs and reasonable individuals understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received payment and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCES

Plaintiff Womack-Devereaux's Experience

180. Plaintiff Womack-Devereaux is a McLaren Health patient and Data Breach victim.

181. As a condition of treatment with McLaren Health, Plaintiff Womack-Devereaux provided it with her Sensitive Information. McLaren Health used that Sensitive Information to facilitate its treatment of Plaintiff Womack-Devereaux and required Plaintiff Womack-Devereaux to provide that Sensitive Information to obtain treatment and care.

182. Plaintiff Womack-Devereaux provided her Sensitive Information to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

183. Plaintiff Womack-Devereaux does not recall ever learning that her Sensitive Information was compromised in a data breach incident, other than the breach at issue in this case.

184. Defendant deprived Plaintiff Womack-Devereaux of the earliest opportunity to guard herself against the Data Breach's effects by its continued failure to notify her of the Breach.

185. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Womack-Devereaux's Sensitive Information for theft by cybercriminals and sale on the dark web.

186. As a result of Defendant's web Breach Notice, Plaintiff Womack-Devereaux spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

187. Plaintiff Womack-Devereaux has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff Womack-Devereaux fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

188. Plaintiff Womack-Devereaux has and is experiencing feelings of anxiety, 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.

189. Plaintiff Womack-Devereaux has suffered actual injury in the form of damages to and diminution in the value of their Sensitive Information – a form of intangible property that Plaintiff Womack-Devereaux entrusted to Defendant, which was compromised in and as a result of the Data Breach.

190. Plaintiff Womack-Devereaux has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

191. Indeed, following the Data Breach, Plaintiff Womack-Devereaux has experienced

an increase in phishing calls and texts, suggesting that her Sensitive Information is now in the hands of cybercriminals.

192. Once an individual's Sensitive Information is for sale and access on the dark web, as Plaintiff Womack-Devereaux's Sensitive Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised data to gather and steal even more information.⁶⁵ On information and belief, the phishing call and texts Plaintiff Womack-Devereaux is experiencing was made possible as a result of Defendant's Data Breach and the subsequent exposure of Plaintiff Womack-Devereaux's Sensitive information to cybercriminals.

193. Plaintiff Womack-Devereaux has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Ranney's Experience

194. Plaintiff Ranney is a McLaren Health patient and Data Breach victim.

195. As a condition of treatment with McLaren Health, Plaintiff Ranney provided it with her Sensitive Information. McLaren Health used that Sensitive Information to facilitate its treatment of Plaintiff Ranney and required Plaintiff Ranney to provide that Sensitive Information to obtain treatment and care.

196. Plaintiff Ranney provided her Sensitive Information to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

197. Plaintiff Ranney has only ever had her Sensitive Information compromised in the McLaren data breach incident which occurred in or around October 2023.

⁶⁵ What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-dohackers-do-with-stolen-information> (last visited January 9, 2024).

198. Defendant deprived Plaintiff Ranney of the earliest opportunity to guard herself against the Data Breach's effects by its continued failure to notify her of the Breach.

199. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Ranney's Sensitive Information for theft by cybercriminals and sale on the dark web.

200. As a result of Defendant's web Breach Notice, Plaintiff Ranney spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

201. Plaintiff Ranney has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff Ranney fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

202. Plaintiff Ranney has and is experiencing feelings of anxiety, 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.

203. Indeed, following the Data Breach, Plaintiff Ranney has been unable to schedule her treatment appointments due to McLaren Health's ongoing inability to resume normal patient portal functions.

204. Plaintiff Ranney has suffered actual injury in the form of damages to and diminution in the value of their Sensitive Information – a form of intangible property that Plaintiff Ranney entrusted to Defendant, which was compromised in and as a result of the Data Breach.

205. Plaintiff Ranney has suffered imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

206. Once an individual's Sensitive Information is for sale and access on the dark, web, as Plaintiff Ranney's Sensitive Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised data to gather and steal even more information.⁶⁶ On information and belief, the phishing call and texts Plaintiff Ranney is experiencing was made possible as a result of Defendant's Data Breach and the subsequent exposure of Plaintiff Ranney's Sensitive information to cybercriminals.

207. Plaintiff Ranney has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Gries's Experience

208. Plaintiff Kayle Gries is a current employee at McLaren.

209. Plaintiff Gries is also a current patient at McLaren.

210. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

211. As part of her employment, Plaintiff Gries likewise was required to provide McLaren with her Private Information.

212. Upon information and belief, at the time of the 2023 Data Breach, Defendant retained Plaintiff Gries's Private Information in its system. Defendant continued to retain Plaintiff Gries's Private Information at the time of the 2024 Data Breach.

⁶⁶ What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-dohackers-do-with-stolen-information> (last visited January 9, 2024).

213. Plaintiff Gries is very careful about sharing her sensitive Private Information. Plaintiff Gries stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Gries would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

214. Plaintiff Gries was a patient of McLaren, beginning in or around 2022. Plaintiff Gries received a Notice Letter from Defendant regarding the 2023 Data Breach on or around October 2023, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the 2023 Data Breach.

215. Plaintiff Gries was also employed by McLaren beginning in or around October 2023. Plaintiff Gries is a remote worker who relies on McLaren's information and operating systems to conduct her duties and work for McLaren.

216. On August 5, 2024, Plaintiff Gries was notified by McLaren that its systems would be going offline for investigation of an alleged data breach. Due to Plaintiff's remote employment status, she was unable to properly complete assignments or duties for or with the company from her home office. Plaintiff Gries was subsequently notified by McLaren that the company's systems would remain offline for an undisclosed amount of time, barring Plaintiff Gries from fulfilling any duties if she did not travel to the McLaren facility nearest her. Unknown to Plaintiff Gries at the time, McLaren's systemwide shut down would last approximately three weeks.

217. Plaintiff Gries is a resident of Hubbard Lake, Michigan and is approximately 2 hours away from the nearest McLaren location. After Plaintiff Gries identified her concerns about an estimated 4-hour daily drive to and from the nearest McLaren facility, McLaren did not provide Plaintiff Gries with any accommodations or alternatives to continuing her work.

218. Plaintiff Gries was also required to use her three-remaining employer-provided Personal Time Off days while McLaren's systems were offline because she could not reasonably work from a McLaren facility. When Plaintiff Gries ran out of Personal Time Off, McLaren advised her that she could apply for Unemployment Benefits during the time she was unable to work due to McLaren's shutdown of its information and operating systems as a result of the 2024 Data Breach. Plaintiff Gries applied for unemployment benefits, but the benefits she would receive were only a fraction of what Plaintiff Gries could have earned if McLaren's information systems were not shut down due to the possible effects of the 2024 Data Breach. Namely, Plaintiff Gries received \$1,095 in a period where she could have earned approximately \$2,190 for 120 hours of work.

219. Upon information and belief, Plaintiff Gries believes her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the 2024 Data Breach occurring on or around August 5, 2024.

220. As a result of the Data Breaches, Plaintiff Gries made reasonable efforts to mitigate the impact of the Data Breaches, including monitoring data potentially impacted by the Data Breaches. Plaintiff Gries has spent significant time dealing with the Data Breaches—valuable time Plaintiff Gries otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

221. Plaintiff Gries suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

222. Plaintiff Gries further suffered actual injury in the form of lost income due to McLaren's systemwide shutdown which, upon information and belief, was caused by the Data Breaches.

223. Plaintiff Gries also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

224. The Data Breaches have caused Plaintiff Gries to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breaches' occurrence. Plaintiff Gries is especially fearful of identity theft, which she reports thinking like it could happen at *any* time in the future.

225. As a result of the Data Breaches, Plaintiff Gries anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

226. As a result of the Data Breaches, Plaintiff Gries is at a present and continued increased risk of identity theft and fraud for years to come.

Plaintiff Drugich's Experience

227. Plaintiff Cheryl Drugich is a current patient at McLaren.

228. In order to obtain medical services at McLaren, she was required to provide it with

her PII and PHI.

229. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Drugich's Private Information in its system.

230. Plaintiff Drugich is very careful about sharing her sensitive Private Information. Plaintiff Drugich stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Drugich would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

231. Plaintiff Drugich received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Drugich entrusted to McLaren was also compromised in the 2024 Data Breach.

232. As a result of the Data Breaches, Plaintiff Drugich made reasonable efforts to mitigate the impact of the Data Breaches, including monitoring her accounts for fraudulent activity and checking her credit reports for unusual activity. Plaintiff Drugich has spent significant time dealing with the Data Breaches—valuable time Plaintiff Drugich otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

233. Plaintiff Drugich suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the

Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

234. The Data Breaches have caused Plaintiff Drugich to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence.

235. As a result of the Data Breaches, Plaintiff Drugich anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

236. As a result of the Data Breaches, Plaintiff Drugich is at a present and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff Norwood's Experience

238. Plaintiff Janise Norwood is a current patient at McLaren.

239. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

240. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Norwood's Private Information in its system.

241. Plaintiff Norwood is very careful about sharing her sensitive Private Information. Plaintiff Norwood stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Norwood would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

242. Plaintiff Norwood received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Norwood entrusted to McLaren was also compromised in the 2024 Data Breach.

243. As a result of the Data Breaches, Plaintiff Norwood made reasonable efforts to mitigate the impact of the Data Breaches, including replacing impacted debit cards. Plaintiff Norwood has spent significant time dealing with the Data Breaches—valuable time Plaintiff Norwood otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

244. Plaintiff Norwood suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

245. Plaintiff Norwood also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

246. The Data Breaches have caused Plaintiff Norwood to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence.

247. As a result of the Data Breaches, Plaintiff Norwood anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

248. As a result of the Data Breaches, Plaintiff Norwood is at a present and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff Porter's Experience

250. Plaintiff Melissa Porter is a current patient at McLaren.

251. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

252. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Porter's Private Information in its system.

253. Plaintiff Porter is very careful about sharing her sensitive Private Information.

Plaintiff Porter stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Porter would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

254. Plaintiff Porter received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Porter entrusted to McLaren was also compromised in the 2024 Data Breach.

255. As a result of the Data Breaches, Plaintiff Porter made reasonable efforts to mitigate the impact of the Data Breaches, including monitoring her accounts for fraudulent activity, closing financial accounts, and contacting Defendant to obtain more details about the Data Breaches. Plaintiff Porter has spent significant time dealing with the Data Breaches—valuable time Plaintiff Porter otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

256. Plaintiff Porter suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

257. Plaintiff Porter additionally suffered actual injury in the form of a credit account being falsely opened under her name, according to Experian and Credit Karma, which, upon information and belief, was caused by the Data Breaches.

258. Plaintiff Porter further suffered actual injury in the form of experiencing fraudulent charges to her Free Star Financial Credit Union Account, in or about September 2023 and December 2023, which, upon information and belief, was caused by the Data Breaches.

259. Plaintiff Porter also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

260. In addition, Plaintiff Porter suffered injury in the form of being charged for medical services from a facility of Defendant's for services that she did not seek or receive, which, upon information and belief, was caused by the Data Breaches.

261. Moreover, Plaintiff Porter experienced actual injury in the form of her Private Information being disseminated on the dark web, according to Experian and Credit Karma, which, upon information and belief, was caused by the Data Breaches.

262. The Data Breaches have caused Plaintiff Porter to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence. Plaintiff Porter has increased her prescribed medication for anxiety as a result of the Data Breach.

263. As a result of the Data Breaches, Plaintiff Porter anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breaches.

264. As a result of the Data Breaches, Plaintiff Porter is at a present and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff McSkulin's Experience

266. Plaintiff Jamie McSkulin is a current patient at McLaren.

267. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

268. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff McSkulin's Private Information in its system.

269. Plaintiff McSkulin is very careful about sharing her sensitive Private Information. Plaintiff McSkulin stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff McSkulin would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

270. Plaintiff McSkulin received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff McSkulin entrusted to McLaren was also compromised in the 2024 Data Breach.

271. As a result of the Data Breaches, Plaintiff McSkulin made reasonable efforts to

mitigate the impact of the Data Breaches, including replacing impacted debit cards. Plaintiff McSkulin has spent significant time dealing with the Data Breaches—valuable time Plaintiff McSkulin otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

272. Plaintiff McSkulin suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

273. Plaintiff McSkulin further suffered actual injury in the form of experiencing fraudulent charges to her Team One Credit Union debit card, for approximately \$150, which, upon information and belief, was caused by the Data Breaches.

274. Plaintiff McSkulin also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

275. The Data Breaches have caused Plaintiff McSkulin to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence. Plaintiff McSkulin is especially

fearful of identity theft, which she reports thinking like it could happen at *any* time in the future.

276. As a result of the Data Breaches, Plaintiff McSkulin anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

277. As a result of the Data Breaches, Plaintiff McSkulin is at a present and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff Wells's Experience

279. Plaintiff Tamyra Ejuan Wells is a current patient at McLaren.

280. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

281. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Wells's Private Information in its system.

282. Plaintiff Wells is very careful about sharing her sensitive Private Information. Plaintiff Wells stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Wells would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

283. Upon information and belief, Plaintiff Wells's PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the Data Breaches.

284. As a result of the Data Breaches, Plaintiff Wells made reasonable efforts to mitigate

the impact of the Data Breaches, including monitoring her accounts for fraudulent activity, researching the Data Breaches, and changing passwords. Plaintiff Wells has spent significant time dealing with the Data Breaches—valuable time Plaintiff Wells otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

285. Plaintiff Wells suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

286. Plaintiff Wells also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

287. The Data Breaches have caused Plaintiff Wells to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence.

288. As a result of the Data Breaches, Plaintiff Wells anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breaches.

289. As a result of the Data Breaches, Plaintiff Wells is at a present and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff Beasley's Experience

291. Plaintiff Ashley Beasley is a former patient at McLaren.

292. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

293. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Beasley's Private Information in its system.

294. Plaintiff Beasley is very careful about sharing her sensitive Private Information. Plaintiff Beasley stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Beasley would not have entrusted Private Information to Defendant had she known of Defendant's inadequate data security policies.

295. Plaintiff Beasley received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Beasley entrusted to McLaren was also compromised in the 2024 Data Breach.

296. As a result of the Data Breaches, Plaintiff Beasley made reasonable efforts to

mitigate the impact of the Data Breaches, including monitoring her accounts for fraudulent activity, changing passwords, and contacting banks regarding fraudulent activity. Plaintiff Beasley has spent significant time dealing with the Data Breaches—valuable time Plaintiff Beasley otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

297. Plaintiff Beasley suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

298. Plaintiff Beasley additionally suffered actual injury in the form of two attempts to open credit cards falsely under her name at Capital One and Citi Bank, which, upon information and belief, was caused by the Data Breaches.

299. Plaintiff Beasley further suffered actual injury in the form of experiencing a fraudulent attempt to agree to be bound by a lease under her name by a caller in Atlanta, Georgia who sought to obtain a copy of her mortgage company so that it could be sent to a leasing company, which, upon information and belief, was caused by the Data Breaches, and which has caused her to expend time and effort in contesting and mitigating the impact of this attempted

fraud, and which, additionally, has caused Plaintiff Beasley stress and anxiety.

300. Plaintiff Beasley also suffered actual injury in the form of experiencing suspicious activity to her Equifax account, forcing her to place a security freeze and fraud alert on her account. Upon information and belief, this suspicious activity was caused by the Data Breaches.

301. Plaintiff Beasley also suffered actual injury in the form of hard inquiries and other suspicious activity on her Experian account, forcing her to place a security freeze on her personal credit report. Upon information and belief, these hard inquiries and suspicious activity was caused by the Data Breaches.

302. Plaintiff Beasley also suffered actual injury in the form of experiencing suspicious activity on her TransUnion credit file, forcing her to place a fraud alert and security freeze on her file. Upon information and belief, this suspicious activity was caused by the Data Breaches.

303. In addition, Plaintiff Beasley suffered injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

304. Moreover, Plaintiff Beasley experienced actual injury in the form of her Private Information being disseminated on the dark web, which, upon information and belief, was caused by the Data Breaches.

305. The Data Breaches have caused Plaintiff Beasley to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence. Plaintiff Beasley's increased anxiety has caused her to lose sleep, as a result of the Data Breaches.

306. As a result of the Data Breaches, Plaintiff Beasley anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by

the Data Breaches.

307. As a result of the Data Breaches, Plaintiff Beasley is at a present and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff Turri's Experience

309. Plaintiff Kyle Turri is a former patient at Defendant.

310. In order to obtain medical services at McLaren, he was required to provide it with his PII and PHI.

311. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Turri's Private Information in its system.

312. Plaintiff Turri is very careful about sharing his sensitive Private Information. Plaintiff Turri stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Turri would not have entrusted his Private Information to Defendant had he known of Defendant's inadequate data security policies.

313. Plaintiff Turri received a Notice Letter from Defendant, informing him that his PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Turri entrusted to McLaren was also compromised in the 2024 Data Breach.

314. As a result of the Data Breaches, Plaintiff Turri made reasonable efforts to mitigate

the impact of the Data Breaches, including contacting Coinbase, filing a police report, researching the Data Breaches, filing a FTC identity theft report, contacting credit bureaus to place freezes on his accounts, and going to banks to place alerts on his accounts. Plaintiff Turri has spent significant time dealing with the Data Breaches—valuable time Plaintiff Turri otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

315. Plaintiff Turri suffered actual injury from having his Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

316. Plaintiff Turri further suffered actual injury in the form of experiencing a fraudulent account being opened under his name and then the debit card being used to withdraw approximately \$9,000 from his Coinbase account in or about August 2023. Upon information and belief, this unauthorized transaction was caused by the Data Breaches.

317. Plaintiff Turri also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

318. The Data Breaches have caused Plaintiff Turri to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the respective Data Breaches' occurrence.

319. As a result of the Data Breaches, Plaintiff Turri anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

320. As a result of the Data Breaches, Plaintiff Turri is at a present and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff Montgomery's Experience

322. Plaintiff Janie Montgomery is a patient at Defendant.

323. In order to obtain medical services at Defendant, she was required to provide her Private Information to Defendant.

324. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Montgomery's Private Information in its system.

325. Plaintiff Montgomery is very careful about sharing her sensitive Private Information. Plaintiff Montgomery stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Montgomery would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

326. Plaintiff Montgomery received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2024 Data Breach.

327. As a result of the 2024 Data Breach, Plaintiff Montgomery made reasonable efforts to mitigate the impact of the 2024 Data Breach. Plaintiff Montgomery has spent significant time dealing with the 2024 Data Breach—valuable time Plaintiff Montgomery otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

328. Plaintiff Montgomery suffered actual injury from having her Private Information compromised as a result of the 2024 Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the 2024 Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the 2024 Data Breach; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

329. Plaintiff Montgomery also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the 2024 Data Breach.

330. The 2024 Data Breach has caused Plaintiff Montgomery to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of

key details about the 2024 Data Breach's occurrence.

331. As a result of the 2024 Data Breach, Plaintiff Montgomery anticipates spending even more time and money, on an ongoing basis, to try to mitigate and address harms caused by the 2024 Data Breach.

332. As a result of the 2024 Data Breach, Plaintiff Montgomery is at a present and continued increased risk of identity theft and fraud for years to come.

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

CLASS ACTION ALLEGATIONS

334. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to MCR 3.501.

335. Specifically, Plaintiffs propose the following class definition, subject to amendment as appropriate:

All persons in the United States whose Personally Identifying Information and/or Protected Health Information was compromised in either of the two Data Breaches disclosed by McLaren (on or about November 9, 2023, and on or about June 20, 2025).

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

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

338. The proposed Class meets the criteria for certification under MCR 3.501 and FR

Civ P 23(a), (b)(2), and (b)(3).

339. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of such persons is currently unknown to Plaintiffs and exclusively in the possession of McLaren, the previous 2023 McLaren data breach involved the Private Information of at least 2.5 million persons, and thus it is reasonable to project a similar number of persons are impacted here.⁶⁷ Thus, the Class is sufficiently numerous to warrant certification.

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

- a. Whether Defendant engaged in the conduct alleged herein;
- b. Whether Defendant's conduct violated the FTCA and/or HIPAA;
- c. When Defendant learned of the Data Breaches;
- d. Whether Defendant's responses to the Data Breaches were adequate;
- e. Whether Defendant unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;
- f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breaches;
- g. Whether Defendant's data security systems prior to and during the Data Breaches complied with applicable data security laws and regulations;
- h. Whether Defendant's data security systems prior to and during the Data Breaches were consistent with industry standards;
- i. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

⁶⁷ <https://www.databreachtoday.com/group-claims-stole-25-million-patients-data-in-attack-a-23212> (last accessed August 8, 2024).

- j. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- k. Whether hackers obtained Class Members' Private Information via the Data Breaches;
- l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breaches to Plaintiffs and Class Members;
- m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breaches to Plaintiffs and Class Members;
- n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;
- p. Whether Defendant's conduct was negligent;
- q. Whether Defendant was unjustly enriched;
- r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

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

theories.

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

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

344. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find the cost of litigating their individual claims to be prohibitively high and would thus 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, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

345. Class certification is also appropriate under MCR 3.501 and FR Civ P 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to Class Members such

that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

346. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiffs and the Class)

347. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

348. Defendant requires its patients, employees, contractors, and other affiliated persons, including Plaintiffs and Class Members, to submit non-public PII and PHI in the ordinary course of providing its medical services and employment.

349. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its patients and employment opportunities, which solicitations and services affect commerce.

350. Plaintiffs and Class Members entrusted Defendant with their Private Information and understood that Defendant would safeguard their information.

351. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed. Defendant also was specifically on notice of the increased threat of data breaches for healthcare providers.

352. By assuming the responsibility to collect and store this data, and in fact doing

so, and sharing it and using it for commercial gain, Defendant had a reasonable duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members’ Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant’s duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach. Additionally, Defendant’s duty is based on the requirements of MCL 500.1406 as a healthcare corporation operating in the State of Michigan.

353. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 USC § 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.

354. Defendant’s duty to use reasonable security measures under HIPAA required Defendant to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 CFR § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.

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

356. 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, employees, and contractors. That special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential Private Information, a necessary part of being patients, employees, and contractors of Defendant. Moreover, Defendant was in an exclusive position to know the extent of its data security capabilities and to detect and prevent the Data Breaches.

357. 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.

358. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

359. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information that it was no longer required to retain pursuant to regulations.

360. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breaches.

361. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

362. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect

Class Members' Private Information. Defendant's specific negligent acts and omissions include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- f. Failing to remove former patients' Private Information that it was no longer required to retain pursuant to regulations; and
- g. Failing to timely and adequately notify Class Members about the Data Breaches' occurrences and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

363. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

364. Plaintiffs and Class Members are within the class of persons that the FTC Act and HIPAA were intended to protect.

365. The harm that occurred as a result of the Data Breaches is the type of harm the FTC Act and HIPAA were intended to guard against.

366. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

367. 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 Plaintiffs and Class Members.

368. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

370. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

371. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and Class Members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

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

373. Plaintiffs and Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

374. Defendant was in a position to protect against the harm suffered by Plaintiffs

and Class Members as a result of the Data Breaches.

375. Defendant's duty extended to protecting Plaintiffs and Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

376. Defendant has admitted that its information systems were breached by an authorized actor on at least two separate occasions.

377. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the Private Information of Plaintiffs and Class Members would not have been compromised.

378. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

379. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breaches; (vii) lost employment opportunities; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

380. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

381. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, 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 Private Information in its continued possession.

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

383. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

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

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

385. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

386. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of receiving medical services or employment opportunities from Defendant.

387. Plaintiffs and Class Members entrusted their Private Information to Defendant. Defendant accepted Plaintiffs' and Class Members' Private Information for the purpose of providing services and employment opportunities for Plaintiffs and Class Members, thereby entering an implied contract whereby Defendant became obligated to reasonably safeguard Plaintiffs' and Class Members' Private Information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

388. Implicit in the agreement between Defendant and Plaintiffs and Class Members to provide Private Information, was Defendant's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

389. The mutual understanding and intent of Plaintiffs and Class Members on the one

hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

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

391. In accepting the Private Information of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

392. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breaches.

393. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

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

395. Plaintiffs and Class Members paid money to or undertook employment opportunities with Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

396. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

397. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of Defendant's implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

398. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

399. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information, and by failing to timely delete certain Private Information, and by failing to provide accurate notice that Private Information was compromised as a result of the August 2024 Breach.

400. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

401. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breaches.

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

COUNT III
Breach of Express Contract
(On Behalf of Plaintiffs and the Class)

403. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

404. As discussed above, Defendant affirmatively agreed to protect the security of the

PII and PHI provided to it by its patients. These express representations appeared in McLaren's Compliance Program and Resources page, its Standards of Conduct, its Notice of Privacy Protection, and its Privacy Policy.

405. Defendant's data security promises were a material term of Plaintiffs' and Class Members' agreement to utilize a McLaren hospital for medical services or agree to undertake employment.

406. Defendant breached its express contractual obligations to reasonably protect and secure the PII and PHI of Plaintiffs and Class Members.

407. Defendant's breaches caused damages to Plaintiffs and Class Members, including nominal damages.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

408. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

409. This count is pleaded in the alternative to Plaintiffs' breach of implied and express contract claims above (Count II and Count III).

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

411. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in

the form of their Private Information as well as payments made or generated by them or on their behalf as a necessary part of their receiving or providing healthcare services. Defendant accepted and realized that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

412. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

413. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members and/or the revenue generated due in part to Plaintiffs and 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.

414. Defendant, however, diverted funds intended to be applied towards data security to its own profit and failed to adequately fund its data security program sufficient to secure Plaintiffs' and Class Members' Private Information from unauthorized access and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

415. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

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

417. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to

Defendant.

418. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs 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 and the safety of their Private Information.

419. Under the principles of equity and good conscience, Defendant should not be permitted to retain the amount that Plaintiffs and Class Members were underpaid, nor retain the money wrongfully obtained from Plaintiffs and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

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

421. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (vii) lost employment opportunities; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse;

and (b) remains backed up 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.

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

423. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that Defendant unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services and/or Plaintiffs and Class Members were underpaid by and through their employment services that they provided to Defendant.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiffs and Plaintiffs' counsel to represent Plaintiffs and 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 Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breaches;
- D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

- iii. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
- iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;
- v. Prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;
- vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. Requiring Defendant to conduct regular database scanning and securing checks;
- xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
- xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. Requiring Defendant to implement a system of tests to assess its respective patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' compliance

with Defendant's policies, programs, and systems for protecting personal identifying information;

- xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and
 - xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
 - xvii. Appointing a qualified and independent third party assessor, for a period of ten years, to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.
- E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
 - F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and 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.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: December 1, 2025

Respectfully submitted,

/s/ Emily E. Hughes

E. Powell Miller (P39487)

Emily E. Hughes (P68724)

THE MILLER LAW FIRM, P.C.

950 West University Drive, Ste. 300

Rochester, MI 48307

Tel: (248) 841-2200

epm@millerlawpc.com

eeh@millerlawpc.com

Gary M. Klinger*

MILBERG, PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

T: (866) 252-0878

gklinger@milberg.com

Benjamin F. Johns

Samantha E. Holbrook

SHUB JOHNS & HOLBROOK LLP

Four Tower Bridge

200 Barr Harbor Drive, Suite 400

Conshohocken, PA 19428

T: (610) 477-8380

bjohns@shublawyers.com

sholbrook@shublawyers.com

Interim Co-Lead Counsel

Samuel J. Strauss*

Raina Borelli (*pro hac vice*)

STRAUSS BORRELLI PLLC

980 N. Michigan Avenue, Suite 1610

Chicago, IL 60611

(872) 263-1100

sam@straussborrelli.com

raina@straussborrelli.com

Additional Plaintiffs' Counsel

****Pro Hac Vice Application Forthcoming***

CERTIFICATE OF SERVICE

I hereby certify that on December, I caused to be served a copy of the forgoing document(s) by filing the same with the Court via hand delivery and via electronic mail to Defense Counsel via their e-mails of record as follows:

tlowe@mcdonaldhopkins.com
cdean@mcdonaldhopkins.com

/s/ Gregory A. Mitchell
Gregory A. Mitchell (P68723)