IN THE UNITED STATES DISTRICT COURT
FOR THE EATERN DISTRICT OF MICHIGAN

MELISSA PORTER,
on behalf of herself and all individuals similarly situated,

Plaintiff,

v.

MCLAREN HEALTH CARE CORPORATION,

Defendant.

Case No. 2:23-cv-12939

TRIAL BY JURY DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Melissa Porter, individually and on behalf of all others similarly situated, brings this action against McLaren Health Care Corporation ("McLaren" or "Defendant"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

SUMMARY OF THE CASE

1. McLaren is a fully integrated health care delivery system with an annual revenue of $6.6 billion encompassing an extensive network across Michigan that includes 14 hospitals with a total bed capacity of 2,624 and supported by a team of 490 physicians. McLaren employs 28,000 full-time staff and maintains contractual relationships with 113,000 providers.

2. On or about August 22, 2023, McLaren became aware of suspicious activity related to its computer systems. McLaren's investigation determined that there was unauthorized access to McLaren's network between July 28, 2023 and August 23, 2023.

3. On October 10, 2023, McLaren announced that it had experienced a massive data breach (the "Data Breach") on August 31, 2023, resulting in the disclosure and theft of approximately 2.2 million individuals' highly sensitive personal identifiable information ("PII") and health information ("protected health information" or "PHI"). Plaintiff's PII and PHI was stolen in the breach.

4. Although McLaren announced the breach on October 10, 2023, it waited nearly a month later (November 9, 2023) and well over two months after the breach itself to announce on its website that an unauthorized threat actor accessed the following data: full name, social security number, health insurance information, date of birth, billing or claims information, diagnosis, physician information, medical record number, Medicare/Medicaid information, prescription/medication information, and diagnostic results and treatment information.

5. A cyber-criminal group called ALPHV/BlackCat has taken responsibility for the attack and theft on McLaren's network, has threatened to release the information if McLaren does not pay a ransom, and has even posted excerpts of the data on the dark web.

6. For years, McLaren has directly and indirectly collected highly sensitive information from its own clients and the customers of its partner health insurance organizations.

7. As a result of the Data Breach, over two million people, including Plaintiff, had their PII and PHI compromised and now have their data being sold on the dark web.

8. The Data Breach was a direct result of McLaren's deficient cybersecurity practices, and the wealth of information and warnings available to McLaren makes its failures all the more egregious.

9. Taking reasonable, standard precautions against cybercrime and data breaches is a fundamental part of doing business in the modern age. By collecting, maintaining, and earning revenue from Plaintiff's and the class members' PII and PHI, McLaren was required by law to exercise

reasonable care and comply with industry and statutory requirements to protect that information—and it failed to do so.

10. McLaren's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence. McLaren disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement proper and reasonable measures to safeguard its customers' PII and failing to take available and necessary steps to prevent unauthorized disclosure of that data.

11. The highly sensitive information exfiltrated in the Data Breach includes, but is not limited to, full name, social security number, health insurance information, date of birth, billing or claims information, diagnosis, physician information, medical record number, Medicare/Medicaid information, prescription/medication information, and diagnostic results and treatment information.

12. Even though McLaren's dereliction of duty led to the Data Breach, Plaintiff and the other victims will bear the burdens of McLaren's negligence for years to come.

13. The costs of the Data Breach, and the sensitivity of the data stolen, cannot be overstated. Criminals can use victims' names, birth dates, social security numbers, and addresses to open new financial accounts, incur charges in credit, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it.[1] Any one of these instances of identity theft can have devastating consequences

[1] *See, e.g.*, *Report to Congressional Requesters*, United States Government Accountability Office (June 2007), http://www.gao.gov/assets/270/262899.pdf; Melanie Lockert, *How do hackers use your information for identity theft?*, CreditKarma (Oct. 1, 2021), https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information; Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS (May 14, 2020), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it; Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, LifeLock by Norton (Feb. 4, 2021), https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft.

for the victim— causing years of often irreversible damage to their credit scores, financial stability, and personal security.

14. Likewise, the exposure of PHI puts Plaintiff and the class members at imminent risk for medical identity theft, especially given the high demand and value of Medicare identification numbers on the dark web.[2] Medical identity theft poses an even more critical threat to victims— medical fraud could lead to loss of access to necessary healthcare if fraudulent activity uses up their paid-for insurance benefits or substantial medical debt.

15. Due to the highly valuable nature of PHI, the FBI has even warned healthcare providers that they are likely to be the targets of cyberattacks like the attack that caused the Data Breach.[3]

16. Plaintiff and the class are at imminent, certain risk for identity theft because of the nature of the PII and PHI exposed.

17. The type of PII and PHI stolen because of McLaren's impermissibly lax data security practices resulted in Plaintiff and the class members becoming imminently at risk for identity or medical identity theft, but McLaren maximized the harm inflicted by waiting more than two months before notifying its effected customers that their highly sensitive, private information was stolen by and in the hands of sophisticated cybercriminals.

18. Plaintiff and class members have suffered numerous injuries as a direct and proximate result of McLaren's conduct. These injuries include: (i) lost value of PII/PHI, a form of property that McLaren obtained from Plaintiff and class members; (ii) out-of-pocket expenses associated with

---

[2] *What to Know About Medical Identity Theft*, Federal Trade Commission (May 2021), https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

[3] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, Reuters (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their PII/PHI; (iii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain risk that unauthorized persons will access and abuse Plaintiff's and class members' highly sensitive PII/PHI that is available on the dark web; (v) the continued and certain increased risk that the PII/PHI that remains in McLaren's possession is subject to further unauthorized disclosure for so long as McLaren fail to undertake proper measures to protect the PII; and (vi) theft of their PII/PHI and the resulting loss of privacy rights in that information.

19. Further, malicious actors will often wait months, or even years, to use stolen PII/PHI to lower chances of detection by the victim or temporary credit monitoring assistance. This means that Plaintiff or the class members could be victims of multiple instances of identity theft as a result of this single breach. While Plaintiff and the class members are already at imminent risk for identity and medical identity theft, such risk will continue, possibly indefinitely, as a direct and foreseeable result of McLaren's negligence. Plaintiff and class members thus have both cognizable and redressable past injuries and a continuing interest in ensuring that their PII and PHI are and remains safe, and they should be entitled to damages and injunctive and other equitable relief.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than McLaren. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

21. This Court has personal jurisdiction over McLaren as its headquarters and principal place of business is in Grand Blanc, Michigan.

22. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and McLaren conducts substantial business in this District.

DEFENDANT MCLAREN

23. McLaren is a nonprofit healthcare corporation incorporated in the State of Michigan. McLaren manages a primary care physician network, commercial and Medicaid HMOs, and assisted living facilities, and provides visiting nurse/home health care and hospice services, which includes over 300 facilities, including a dozen regional hospitals and a network of cancer, dialysis, imaging, and surgery centers across the state of Michigan.

NAMED PLAINTIFF

24. Plaintiff Melissa Porter is a resident and citizen of Chesterfield, Michigan. Prior to the Data Breach, Plaintiff used McLaren health services under coverage of a health insurance plan. Specifically, she was a patient at McLaren Macomb Hospital on several occasions from 2019-2023.

25. On November 17, 2023, Plaintiff received a letter in the mail from McLaren (dated November 9, 2023) informing her of the Data Breach. The letter stated that through McLaren's investigative "process, which concluded on October 10, 2023," it learned that "information pertaining to you may have been included in the potentially impacted files." The letter went on to dishonestly claim that there is "currently no evidence that your information has been misused." The letter nowhere acknowledged that ALPHV/BlackCat has taken credit for the Data Breach, has threatened to release the data, and has even posted excerpts of the data on the dark web.

26. Upon information and belief, Plaintiff has taken reasonable steps to keep her PII/PHI confidential and secure. Following the Data Breach, where Plaintiff's PII and/or PHI (including her

social security number) was exfiltrated, Plaintiff has spent considerable time and effort regularly monitoring her accounts to detect fraudulent activity in order to mitigate against potential harm, especially because the leak of her highly sensitive information means that she is substantially at risk for identity theft in the future. With her highly sensitive information now in the hands of a criminal group seeking to profit off of her illegally obtained PII and/or PHI, Plaintiff is at substantial and imminent risk of future harm, including but not limited to identity theft.

FACTUAL ALLEGATIONS

A. McLaren's Use of Patient Data

27. McLaren operates Michigan's largest network of cancer centers and providers, anchored by the Karmanos Cancer Institute, one of only 53 National Cancer Institute-designated comprehensive cancer centers in the U.S. McLaren has 28,000 full, part-time and contracted employees and more than 113,000 network providers throughout Michigan, Indiana and Ohio.[4]

28. McLaren requires its patients to provide PII/PHI in order to avail themselves to McLaren's services.

29. Upon information and belief, McLaren also receives and maintains the PHI of the patients and employees of its partners, including full name, social security number, health insurance information, date of birth, billing or claims information, diagnosis, physician information, medical record number, Medicare/Medicaid information, prescription/medication information, and diagnostic results and treatment information.

30. McLaren routinely collects PII, including but not limited to, social security numbers, payment card information, billing, and claims and location information.[5]

---

[4] McLaren, *About McLaren Health Care*, https://www.mclaren.org/main/about-mclaren-health-care (las visited Nov. 17, 2023).

[5] *See McLaren Health Care Web Privacy Policy*, https://www.mclaren.org/main/web-privacy-policy (last

31. By taking and collecting Plaintiff and the class members' sensitive information, McLaren agreed to use reasonable safety and security measures in line with industry standards.

32. By obtaining, collecting, receiving, and storing Plaintiff's and Class Members' PII/PHI McLaren assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' PII/PHI from unauthorized disclosure.

33. In its Privacy Policy, McLaren promises patients and customers that it will take "reasonable measures to protect Personally Identifiable Information."[6]

B. The Data Breach

34. On or about August 22, 2023, McLaren became aware of suspicious activity related to its computer systems. It determined that there was unauthorized access to McLaren's network between July 28, 2023 and August 23, 2023. On August 31, 2023, McLaren learned the unauthorized actor had the ability to acquire certain information stored on the network during the period of access.

35. In fact, on October 10, 2023, McLaren announced that it had experienced the Data Breach, which resulted in the disclosure and theft of nearly 2.2 million individuals' highly sensitive PII and PHI. Based on the letter she received from McLaren on November 17, 2023, Plaintiff's PII and PHI was stolen in the breach.

36. Upon information and belief, ALPHV/BlackCat ransomware group hackers not only accessed and downloaded McLaren's customers' sensitive personal information, but also moved across McLaren's other networks and systems to access vast troves of personal information. ALPHV/BlackCat even claims that it still has access to McLaren's network.

---

modified Mar. 24, 2022 and last visited on November 17, 2023).

[6] *Id.*

37. Upon information and belief, the ALPHV/BlackCat ransomware group issued a ransom demand to McLaren and threatened to leak customer data unless paid.

38. On information and belief, Plaintiff's and the class members' PII/PHI was unprotected and unencrypted, and therefore easily accessible for unauthorized access and exfiltration.

39. Although McLaren's system was compromised by no later than August 31, 2023, it did not acknowledge that its servers had been hacked for at least 40 more days (on October 10, 2023), and it did not mail a letter notifying affected patients of the compromise of their most sensitive PII/PHI until November 9, 2023—nearly another month later. Indeed, the length of time the Data Breach went unnoticed and undetected by McLaren is astonishing.

C. McLaren's Knowledge of Cyber Security Threats

40. At all relevant times, McLaren was well-aware, or reasonably should have been aware, that the PII/PHI collected, maintained, and stored in its servers is highly sensitive, susceptible to attack, and could be used for malicious purposes by third parties, such as identity theft, fraud and other misuse.

41. The frequency and prevalence of attacks make it imperative for entities to routinely and constantly monitor for exploits and attacks, and regularly update its software and security procedures.

42. McLaren was fully aware that the healthcare benefits industry is a prime target for cyber threats.[7] High profile data breaches in for similar industry leaders in healthcare put them on notice of this fact, *e.g.*, Trinity Health (3.3 million patients, May 2020); Shields Healthcare Group (2

[7] *See, e.g.*, Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, Reuters (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

million patients, March 2022). Between 2020 and 2021, attacks on the healthcare industry increased 71%, making it the fifth most common industry targeted by cyberattacks.[8]

43. McLaren also knew or should have known of the threat that the ALPHV/BlackCat ransomware and similar other groups posed to its patients. The healthcare industry is also the primary target for the ALPHV/BlackCat group. The Department of Health and Human Services even issued an alert in January 2023 warning the healthcare sector of potential attacks from this very hacking group.[9] ALPHV/BlackCat has previously targeted file transfer services as a means to target the healthcare sector.[10]

D. McLaren Breached Its Duties to Plaintiff

44. As any entity collecting and maintaining Plaintiff's and the class members' highly sensitive personal information, McLaren had a duty to exercise reasonable care and comply with applicable industry standards and statutory security requirements to protect their information.

45. McLaren's HIPAA Rights disclosure even provides that they "are required by law to maintain the privacy and security of your protected health information."[11]

46. Despite holding PII/PHI for millions of individuals, McLaren failed to adopt reasonable data security measures to prevent and detect unauthorized access to its highly sensitive databases, putting its customers' highly sensitive information at risk.

---

[8] Check Point Research Team, *Check Point Research: Cyber Attacks Increased 50% Year over Year*, Check Point (Jan. 10, 2022), https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/.

[9] Office of Information Security, United States Department of Health and Human Services, *Royal & BlackCat Ransomware: The Threat to the Health Sector* (Jan. 12, 2023), https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf.

[10] *Id.*

[11] McLaren Health Care Web Privacy Policy, https://www.mclaren.org/main/web-privacy-policy (last modified Mar. 24, 2022 and last visited on November 17, 2023).

47. McLaren had the resources to prevent a breach and made significant expenditures to market its supplemental benefits and technology solutions, but neglected to invest adequately in data security, despite the growing number of well-publicized data breaches affecting the healthcare and insurance industries.

48. McLaren failed to properly implement data security practices that were reasonable and compliant with industry standards.

49. On information and belief, McLaren was at all times aware of its obligations and duties to protect Plaintiff's and class members' private information, and aware of the significant repercussions resulting from its failure to do so.

E. McLaren Failed to Comply with Regulatory Requirements and Industry Practices

50. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of PII/PHI.

51. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain personal information, or PII, about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect PII/PHI from unauthorized access. Michigan is one such state and requires that entities like McLaren "to ensure the confidentiality of records containing personal data that may be associated with identifiable members, [and] use reasonable care to secure these records from unauthorized access and to collect only personal data that are necessary for the proper review and payment of claims and for health care operations." Mich. Comp. Laws Ann. § 550.1406.

52. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[12]

53. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[13] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII/PHI that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack 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.

54. The FTC recommends that companies not maintain PII/PHI 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.[14]

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or

---

[12] Federal Trade Commission, *Start With Security* 2 (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[13] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[14] *See* FTC, *Start With Security*, *supra* n. 13.

practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. The FTC interprets Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that failure to restrict access to information[15] and failure to segregate access to information[16] may violate the FTC Act.

57. McLaren's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data (*i.e.*, PII/PHI) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

58. Furthermore, McLaren is required to comply with the HIPAA Privacy Rules and Security Rule, 45 C.F.R. 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 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set the nationwide standards for protecting health information, including health information stored electronically.

59. The Security Rule requires McLaren 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;

---

[15] *In the Matter of LabMD, Inc.*, Dkt. No. 9357, Slip Opinion, at 15 ("Procedures should be in place that restrict users' access to only that information for which they have a legitimate need."), *available at* https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf.
[16] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (companies should use "readily available security measures to limit access between" data storage systems).

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.[17]

60. Pursuant to HIPAA's mandate that McLaren follow "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302, McLaren was required to, at minimum, to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[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 C.F.R. § 164.312(a)(1).

61. McLaren is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

62. Both HIPAA and HITECH obligate McLaren to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient PII. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. §17902.

[17] U.S. Department of Health and Human Services, Summary of the HIPAA Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Nov. 17, 2023).

F. The Effect of the Data Breach on Impacted Customers

63. McLaren's failure to keep Plaintiff's and class members' PII/PHI secure has severe ramifications. Given the sensitive nature of the information stolen in the Data Breach—names, addresses, health information, dates of birth, Social Security Numbers—hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and class members now and into the indefinite future.

64. The data exposed in the Data Breach, including customers' social security numbers, full names, dates of birth, and health insurance information, is highly coveted and valuable on underground or black markets. Upon information and belief, Plaintiff's and the class members' data is already being used as a bargaining chip to extract a ransom from McLaren, and if McLaren does not pay, it will be posted on the dark web or sold on the black market for criminals to use it for identity theft and other nefarious purposes.

65. Cyber criminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.[18] The shelf life for this information is also far longer—while individuals can update their credit card numbers, they are less likely to change their Medicare numbers, health insurance information, or social security numbers.

66. Medicare beneficiary numbers like Plaintiff's are "even more valuable than stolen credit cards," and often result in the filing of false claims for Medicare reimbursement.[19]

---

[18] Federal Trade Commission, *Medical Identity Theft: FAQs for Health Care Providers and Health Plans* 1 (Jan. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.

[19] Melissa D. Berry, *Medicare under attack: Healthcare data breaches increase fraud risks*, Thomson Reuters (Mar. 3, 2023), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-

67. According to the U.S. Government Accountability Office, "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[20]

68. Because of its value and the loss of sensitive health information and social security numbers, future identity theft is certainly impending.

69. Identity thieves can use the PII/PHI to: (a) apply for credit cards or loans (b) purchase prescription drugs or other medical services (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or insurance benefits; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

70. This is especially true for the sensitive PII/PHI compromised in this data breach.

71. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[21]

72. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[22]

---

risk/medicare-fraud-risks/.

[20] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTSGAO-07-737.htm.

[21] Al Pascual, Kyle Marchini & Sarah Miller, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, Javelin (Feb. 6, 2018), https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

[22] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at

73. For class members who had their Social Security Numbers exposed, the unauthorized disclosure can be particularly damaging because, unlike a credit card, Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you shouldn't use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[23]

74. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of a Social Security Number, identity theft victims must spend numerous hours and their own money repairing the impact to their credit.

75. A 2017 Identity Theft Resource Center survey[24] evidences the emotional suffering experienced by victims of identity theft:

---

https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Nov. 17, 2023).

[23] United States Social Security Administration, *Identity Theft and Your Social Security Number* (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[24] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017* (2017),

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.

76. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[25]

77. There may also be a significant time lag between when PII/PHI is stolen and when it is actually misused. According to the U.S. Government Accountability Office ("GAO"), 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.

---

https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf.
[25] *Id.*

As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

78. As the result of the Data Breach, Plaintiff and class members have suffered and/or will suffer or continue to suffer economic loss, a substantial risk of future identity theft, and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- losing the inherent value of their PII;
- losing the value of McLaren's implicit promises of adequate data security;
- identity theft and fraud resulting from the theft of their PII/PHI;
- costs associated with the detection and prevention of identity theft and unauthorized use of their medical and health insurance information;
- costs associated with purchasing credit monitoring and identity theft protection services;
- unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address

[26] United States Government Accounting Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO report number GAO-07-737 (July 5, 2007).

the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

- the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII/PHI being in the possession of one or many unauthorized third parties.

79. Additionally, Plaintiff and class members place significant value in data security.

80. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like McLaren would have no reason to tout its data security efforts to its actual and potential patients.

81. Consequently, had patients known the truth about McLaren's data security practices—that McLaren would not adequately protect and store their data—they would not have entrusted their PII/PHI to McLaren to provide healthcare services. As such, Plaintiff and class members did not receive the benefit of their bargain with McLaren because they paid for a value of services they expected but did not receive.

CLASS ACTION ALLEGATIONS

82. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seek certification of the following nationwide class (the "Class" or the "Nationwide Class"):

> **All persons in the United States whose PII/PHI were compromised in the Data Breach**.

83. The Nationwide Class asserts claims against McLaren for negligence (Count 1), negligence *per se* (Count 2), unjust enrichment (Count 3), and declaratory judgment (Count 4)).

84. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of a Michigan subclass (the "Michigan Subclass") for statutory claim pursuant Michigan Mich. Comp. Laws Ann. § 550.1406 (Count 5), defined as follows:

All persons in Michigan whose PII/PHI were compromised in the Data Breach.

85. Excluded from the Nationwide Class and Michigan Subclass, any entity in which any McLaren has a controlling interest, and McLaren's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each State Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

86. Plaintiff hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

87. Each of the proposed classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

88. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Nationwide Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiff at this time, McLaren has acknowledged that the PII/PHI of approximately 2,192,515 individuals across at least three states were compromised in the Data Breach. Those persons' names and addresses are available from McLaren's records, and class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet notice, and/or published notice.

89. **Predominance of Common Issues**. Fed. R. Civ. P. 23(a)(2) and (b)(3). Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves

common questions of law and fact that predominate over any questions affecting individual class members. The common questions include:

a. Whether McLaren knew or should have known that its servers and configurations were vulnerable to attack;

b. Whether McLaren failed to take adequate and reasonable measures to ensure that its computer, applications, and data systems were protected;

c. Whether McLaren failed to take available steps to prevent and stop the Breach from happening;

d. Whether McLaren owed tort duties to Plaintiff and class members to protect their PII;

e. Whether McLaren owed a duty to provide timely and accurate notice of the Data Breach to Plaintiff and class members;

f. Whether McLaren breached its duties to protect the PII/PHI of Plaintiff and class members by failing to provide adequate data security;

g. Whether McLaren's failure to secure Plaintiff's and class member's PII/PHI in the manner alleged violated federal, state and local laws, or industry standards;

h. Whether McLaren's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to and/or theft of Plaintiff's and class members' PII;

i. Whether McLaren's conduct amounted to violations of state consumer protection statutes;

j. Whether, as a result of McLaren's conduct, Plaintiff and class members face a significant threat of identity theft, harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

k. Whether McLaren should retain the money paid by Plaintiff and class members to protect their PII;

l. Whether McLaren should retain Plaintiff' and class members' valuable PII;

m. Whether, as a result of McLaren's conduct, Plaintiff and class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

90. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiff's claims are typical of other class members' claims because Plaintiff and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

91. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Classes because Plaintiff is a member of the Classes and are committed to pursuing this matter against McLaren to obtain relief for the Classes. Plaintiff has no conflicts of interest with the Classes. Plaintiff's Lead Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the interests of all of the Classes.

92. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means 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. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to Plaintiff and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the class members are relatively small compared to the burden and expense

required to individually litigate their claims against McLaren, and thus, individual litigation to redress McLaren's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

93. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). McLaren, through its uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole.

94. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

95. Finally, all members of the proposed Class are readily ascertainable. McLaren has access to information regarding which individuals were affected by the Data Breach, and has already provided notifications. Using this information, the members of the Class can be identified, and their contact information ascertained for purposes of providing notice to the Class.

CAUSES OF ACTION

COUNT 1
NEGLIGENCE

96. Plaintiff realleges and incorporates herein all previous paragraphs of this Complaint.

97. McLaren acquired and maintained Plaintiff's and class members' sensitive personal information, including their full name, social security number, health insurance information, date of birth, billing or claims information, diagnosis, physician information, medical record number,

Medicare/Medicaid information, prescription/medication information, and diagnostic results and treatment information.

98. By collecting, storing, using, and earning revenue from this data, McLaren had a duty of care to Plaintiff and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing its security systems and data storage architecture to ensure that Plaintiff's and class members' PII/PHI was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely manner; (c) timely acting upon all warnings and alerts, including public information, regarding security vulnerabilities and potential compromise of the compiled data of Plaintiff and millions of class members; and (d) maintaining data security measures consistent with industry standards.

99. McLaren had common law duties to prevent foreseeable harm to Plaintiff and class members. These duties existed because Plaintiff and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and class members would be harmed by the failure to protect their PII/PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, but McLaren also knew that it was more likely than not Plaintiff and other class members would be harmed by such theft.

100. McLaren had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII/PHI that was collected and stored on its servers.

101. McLaren's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of

failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of McLaren's duties.

102. McLaren's duty to use reasonable security measures also arose under HIPAA, under which McLaren was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

103. McLaren knew or should have known that McLaren's server was vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII/PHI.

104. McLaren breached the duties it owed to Plaintiff and class members described above and thus were negligent. McLaren breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII/PHI of Plaintiff and class members; (b) detect the breach while it was ongoing or even promptly after it occurred; and (c) maintain security systems consistent with industry standards.

105. But for McLaren's wrongful and negligent breach of its duties owed to Plaintiff and class members, their PII/PHI would not have been compromised.

106. As a direct and proximate result of McLaren's negligence, Plaintiff and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII/PHI; illegal sale of the compromised PII/PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements,

credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII/PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT 2

NEGLIGENCE *PER SE*

107. Plaintiff realleges and incorporates herein all previous paragraphs of this Complaint.

108. Under the FTC Act, 15 U.S.C. § 45, McLaren had a duty to provide fair and appropriate computer systems and data security practices to safeguard Plaintiff's and class members' sensitive PII/PHI.

109. In addition, under Michigan state data security statutes, McLaren had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and class members' sensitive PII/PHI.

110. McLaren breached its duties to Plaintiff and Class Members, under the FTC Act and the Michigan state data security statutes, by failing to provide fair, reasonable, or appropriate computer systems and data security practices to safeguard Plaintiff's and class members' sensitive PII/PHI.

111. McLaren is covered by HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule, 45 C.F.R Part 160 and Par108501t 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 C.F.R. Part 160 and Part 164, Subparts A and C. HIPAA prohibits unauthorized disclosures of "protected health information," which includes the information at issue here.

112. Plaintiff and Class Members were foreseeable victims of McLaren's violations of the FTC Act, HIPAA, and state data security statutes. McLaren knew or should have known that the

failure to implement reasonable measures to protect and secure Plaintiff's and class members' sensitive PII/PHI would cause damage to Plaintiff and class members.

113. McLaren's failure to comply with the applicable laws and regulations constitutes negligence per se.

114. But for McLaren's violation of the applicable laws and regulations, Plaintiff's and Class Members' Private Information would not have been accessed by unauthorized parties.

115. As a direct and proximate result of McLaren's negligent conduct, Plaintiff and class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT 3

UNJUST ENRICHMENT

116. Plaintiff realleges and incorporates herein all previous paragraphs of this Complaint.

117. Plaintiff and class members have an interest, both equitable and legal, in the PII/PHI that was conferred upon, collected by, and maintained by McLaren and that was ultimately stolen in the Data Breach.

118. McLaren was benefitted by the conferral upon it of the PII/PHI pertaining to Plaintiff and class members and by its ability to retain, use, and earn revenue from that information. McLaren understood that it was in fact so benefitted.

119. McLaren also understood and appreciated that the PII/PHI pertaining to Plaintiff and class members was private and confidential and its value depended upon McLaren maintaining the privacy and confidentiality of that PII/PHI.

120. But for McLaren's willingness and commitment to maintain its privacy and confidentiality, that PII/PHI would not have been transferred to and entrusted with the McLaren.

121. McLaren continues to benefit from its retention and use of the PII/PHI while its value to Plaintiff and class members has been diminished.

122. McLaren also benefitted through its unjust conduct by retaining portions of Plaintiff's and the class members' payments for medical services that it should have used to provide reasonable and adequate data security to protect Plaintiff' and class members' PII.

123. It is inequitable for McLaren to retain these benefits.

124. As a result of McLaren's wrongful conduct as alleged in this Complaint (including, among things, its knowing failure to employ adequate data security measures, its continued maintenance and use of the PII/PHI belonging to Plaintiff and class members without having adequate data security measures, and its other conduct facilitating the theft of that PII), McLaren have been unjustly enriched at the expense of, and to the detriment of, Plaintiff and class members.

125. McLaren's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff' and class members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

126. Under the common law doctrine of unjust enrichment, it is inequitable for McLaren to be permitted to retain the benefits it received, and are still receiving, without justification, from Plaintiff and class members in an unfair and unconscionable manner. McLaren's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

127. The benefits conferred upon, received, and enjoyed by McLaren were not conferred officiously or gratuitously, and it would be inequitable and unjust for McLaren to retain these benefits.

128. Plaintiff has no adequate remedy at law.

129. McLaren is therefore liable to Plaintiff and class members for restitution or disgorgement in the amount of the benefit conferred on McLaren as a result of its wrongful conduct,

including specifically: the value to McLaren of the PII/PHI that was stolen in the Data Breach; the revenue McLaren is receiving from the use of that information; the amounts that Plaintiff and class members were overcharged for their health insurance or supplemental benefits insurance as a result of McLaren's services; and the amounts that McLaren should have spent to provide reasonable and adequate data security to protect Plaintiff's and class members' PII/PHI.

COUNT 4

DECLARATORY JUDGMENT

130. Plaintiff realleges and incorporates herein all previous paragraphs of this Complaint.

131. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

132. An actual controversy has arisen in the wake of the Data Breach regarding McLaren's present and prospective common law and other duties to reasonably safeguard its customers' PII/PHI and whether McLaren is currently maintaining data security measures adequate to protect Plaintiff and class members from further data breaches that compromise their PII. Plaintiff remains at imminent risk that further compromises of their PII/PHI will occur in the future.

133. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. McLaren continues to owe a legal duty to secure consumers' PII/PHI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, HIPAA, the Florida Information Protection Act, and various state statutes;

b. McLaren continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII/PHI.

134. The Court also should issue corresponding prospective injunctive relief requiring McLaren to employ adequate security practices consistent with law and industry standards to protect consumers' PII/PHI

135. If an injunction is not issued, Plaintiff and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at McLaren. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

136. The hardship to Plaintiff and class members if an injunction does not issue exceeds the hardship to McLaren if an injunction is issued. Among other things, if another massive data breach occurs at McLaren, Plaintiff and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to McLaren of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and McLaren has a pre-existing legal obligation to employ such measures.

137. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at McLaren, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose PII/PHI would be further compromised.

COUNT 5

Mich. Comp. Laws Ann. § 550.1406

On Behalf of Plaintiff and the Michigan Subclass

138. Plaintiff realleges and incorporates herein all previous paragraphs of this Complaint.

139. The Nonprofit Health Care Corporation Reform Act ("the Act"), Mich. Comp. Laws Ann. § 550.140 *et seq.*, requires in relevant part that a Michigan nonprofit healthcare corporation "use

reasonable care to secure" members' healthcare records "from unauthorized access" and thereby "ensure the confidentiality of records containing personal data that may be associated with identifiable members." Mich. Comp. Laws Ann. § 550.1406(1).

140. As a nonprofit healthcare corporation incorporated in the State of Michigan and providing healthcare and hospital services in the State, McLaren is and was at all relevant times a "healthcare corporation" as that term is defined in Mich. Comp. Laws Ann. §§ 550.1105(2) and 50.1406.

141. As a person entitled to receive healthcare under a nongroup insurance certificate while obtaining healthcare from McLaren, Plaintiff is an was at all relevant times a "member" as that term is defined in Mich. Comp. Laws Ann. §§ 550.1106(3) and 50.1406.

142. By the acts alleged above, McLaren violated the Act by failing to adequately safeguard Plaintiff's PII/PHI from malicious actors. Considering the number of past data breaches and the sensitivity of the information McLaren possessed, McLaren was aware or should have been aware of the need to implement robust security measures to protect such information. It consciously refused to do so.

143. Accordingly, Plaintiff and each member of the Michigan subclass are entitled to, and seek, damages "for a violation of [the Act] and may recover actual damages or $200.00, whichever is greater, together with reasonable attorneys' fees and costs." § 550.1406(4).

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against McLaren as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and Plaintiff's Lead Counsel to represent the Classes as alleged herein;

b. For injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and class members, including but not limited to an order:

c. Prohibiting McLaren from engaging in the wrongful and unlawful acts described herein;

d. Requiring McLaren 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;

e. Requiring McLaren to delete, destroy and purge the PII/PHI of Plaintiff and class members unless McLaren can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and class members;

f. Requiring McLaren to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff' and class members' PII;

g. Requiring McLaren 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 McLaren's systems on a periodic basis, and ordering McLaren to promptly correct any problems or issues detected by such third-party security auditors;

h. Requiring McLaren to engage independent third-party security auditors and internal personnel to run automated security monitoring;

i. Requiring McLaren to audit, test, and train its security personnel regarding any new or modified procedures;

j. Requiring McLaren to segment data by, among other things, creating firewalls and access controls so that if one area of McLaren's network is compromised, hackers cannot gain access to other portions of McLaren's systems;

k. Requiring McLaren to conduct regular database scanning and securing checks;

l. Requiring McLaren to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII/PHI, as well as protecting the PII/PHI of Plaintiff and class members;

m. Requiring McLaren to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

n. Requiring McLaren to implement a system of testing to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with McLaren's policies, programs and systems for protecting PII/PHI;

o. Requiring McLaren to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor the McLaren's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

p. Requiring McLaren to meaningfully educate all class members about the threats they face as a result of the loss of their PII/PHI to third parties, as well as the steps affected individuals must take to protect themselves;

q. Requiring McLaren to implement logging and monitoring programs sufficient to track traffic to and from McLaren's servers; and

r. For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

s. For an award of statutory damages and punitive or exemplary damages, as allowed by law in an amount to be determined;

t. For an award of restitution or disgorgement, in an amount to be determined;

u. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

v. For prejudgment interest on all amounts awarded; and

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

JURY DEMAND

Plaintiff, on behalf of themselves and the Class of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Date: November 17, 2023

/s/ Hassan A. Zavareei
Hassan A. Zavareei
hzavareei@tzlegal.com
David W. Lawler (application for *pro hac vice* admission forthcoming)
dlawler@tzlegal.com
Glenn E. Chappell (application for *pro hac vice* admission forthcoming)
gchappell@tzlegal.com
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Ave NW, Suite 1010,
Washington, D.C. 20006
Telephone: (202) 973-0900
Facisimile: (202) 973-0950

Counsel for Plaintiff and the Proposed Classes