UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

DAVID WEATHERS, on behalf of himself and others similarly situated, Plaintiff, vs. MCLAREN HEALTH CARE CORPORATION, Defendant.	Case No.: CLASS ACTION COMPLAINT AND JURY DEMAND

I. CLASS ACTION COMPLAINT

Plaintiff DAVID WEATHERS ("Plaintiff"), on behalf of himself and others similarly situated ("the Class"), bring this action against Defendant MCLAREN HEALTH CARE CORPORATION ("McLaren" or "Defendant") for actual damages suffered by Plaintiff and the Class, statutory damages, penalties, restitution, injunctive relief, and for other recovery specified herein for harm caused by McLaren's violations of Michigan consumer and data protection laws, negligent conduct, and breach of contract. Plaintiff alleges upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record, as follows:

II. INTRODUCTION

1. Data security has taken center stage as global losses from cybercrime exceed $1 trillion annually. The global pandemic has made consumers and organizations more vulnerable than ever before to cyber-attacks and increased the importance of strong safeguards against cybercriminals.

2. Because of the highly sensitive nature of the data maintained in their care, healthcare institutions 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. IBM Research reports that healthcare has been the hardest hit industry by cybercrime for twelve consecutive years.

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, 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. When Michigan amended the Nonprofit Health Care Corporation Reform Act (MCL 500.1400, *et seq*.) in 2006, it included a requirement that all health care corporations take care to secure records that include personally identifiable information ("PII") and created a private right of action for a failure to safeguard that data.

4. Responsible institutions have reacted by implementing better training practices, increasing their security workforces, and increasing investment in new and more secure technologies.

5. McLaren is a healthcare corporation is a multi-billion-dollar integrated system of hospitals, surgical centers, and other providers operating primarily in Michigan. Patients entrust it with their most personal information—their healthcare data. Such data can include past medical procedures, chronic health issues, or catastrophic diagnoses.

6. In August 2023, unauthorized users accessed approximately 2.5 million McLaren patient files. Upon accessing the files, these unauthorized users obtained patients' sensitive personal medical information.

7. Rather than alerting patients of the breach right away as required under state law, McLaren said nothing. Patients first learned of the breach when news outlets reported on the hacker organization that publicized its victory in October. The delay caused further harm, allowing the hackers more time to exploit the information.

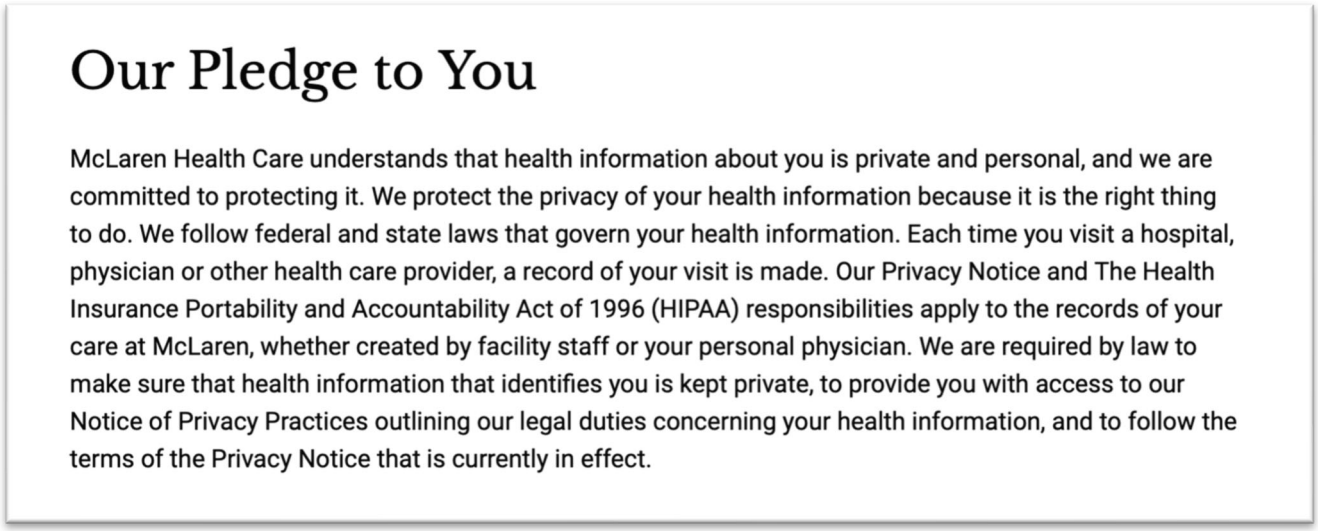
III. FACTUAL ALLEGATIONS

8. McLaren is a regional healthcare conglomerate founded in Flint Michigan in 1919. The system employs nearly 30,000 healthcare workers and claims access to a network of over 100,000 providers at its in-patient treatment, laboratory, diagnostic, surgical, and other

medical facilities. It touts the extraordinary number of patients it treats every year, with over 80,000 patients admitted, 380,000 treated by emergency services, and 250,000 home visits annually.

9. McLaren collects or receives treatment records, lab testing data, demographic information, and payment information from its patients. Patients entrust McLaren with this information, which, by its nature, is highly sensitive and may include their medical histories, current conditions, medications, social security numbers, credit card numbers, and other sensitive PII.

10. Because of the highly sensitive nature of this information, McLaren makes many bold promises to protect patient data. Its Compliance Program and Resources page, for example, make 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 …

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.

11. McLaren is required under state and federal law to maintain patient data in strict confidence. Under the Health Insurance Portability and Accountability Act ("HIPAA") Security Management Process Standard (45 C.F.R. § 164.308), McLaren is required to "implement policies and procedures to prevent, detect, contain, and correct security violations;" and "implement a security awareness and training program for all members of its workforce;" among other things.

12. Additionally, Michigan state laws require McLaren to "use reasonable care to secure [records containing personal data] from unauthorized access." MCL 500.1406(1). It also requires McLaren's Board of Directors to establish a policy that, at a minimum, "assure[s] that no person shall have access to personal data except on the basis of a need to know." MCL 500.1406(2)(c).

13. These internal policies, federal regulations, and state statutes specifically require McLaren to keep its electronic networks and databases containing sensitive patient data secure and to send prompt and appropriate notifications if a breach occurs.

14. McLaren did not keep its pledge to maintain patient privacy. Based on the nature of the breach and the statements of the unauthorized users who gained access to the McLaren networks, Plaintiff alleges on information and belief that McLaren's system lacked simple and almost universal security measures used by healthcare companies, such as 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.

15. McLaren's failure to use these and other industry-standard security measures needlessly exposes patients whose data was stored with McLaren to the risk of data theft.

16. At some point in time before August 31, 2023, McLaren negligently and illegally allowed an unauthorized third-party group called "ALPHV," or "BlackCat," to access patients' data files. The unauthorized user gained access to the McLaren system through a ransomware attack, where malicious software restricted McLaren users from accessing tools. McLaren continued to operate while under attack. But on or before August 31, 2023, according to McLaren, it realized that BlackCat had accessed, manipulated, exfiltrated, and stole 2.5 million patients' personal medical information, including, among other things, their names, dates of service, and medical records. Because of this negligent and illegal conduct, patients' data is now for sale on the dark web.

17. BlackCat was a threat actor known to McLaren at the time the breach occurred and McLaren had been warned of its methods and strategies. In January 2023, the Michigan Department of Health and Human Services' Office of Information Security and Health Sector Cybersecurity Coordination Center issued a joint brief warning entities in the healthcare sector, including McLaren, that ransomware attacks from BlackCat posed a specific threat to the industry. 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' PII.

18. Based on the nature of the breach and the statements of the unauthorized users who gained access to the McLaren networks, Plaintiff alleges on information and belief that McLaren 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.

19. After the breach, McLaren neglected to inform patients of its security failure and the unauthorized theft of their personal medical information for weeks. The first public acknowledgement of the breach was in response to an October 2023 report following the hackers' public claims they had accessed several terabytes of data from the McLaren system relating to 2.5 million patients.

20. To date, McLaren has failed to notify all of the affected patients that their information was released. In total, at least 46 days have passed between McLaren's knowledge of the ransomware attack and its notice to the affected patients.

21. When patients learned of the breach of their medical files by way of reports in the media in October 2023, they were outraged. Their most sensitive information had been for sale to the highest bidder in a criminal auction for more than a month. As a result, the patients experienced and continue to experience anxiety, stress, and anger.

22. Patients have incurred and will continue to incur expenses trying to mitigate their harm. Identity theft protection and credit monitoring services cost consumers as much as $30 per month. Tracking down and containing hacked medical information is even more costly, requiring the use of private investigators and data security professionals. Studies by the National Institute of Standards and Technology show hackers often steal data and then hold it for future use years, or even decades later. Thus, the victims of the McLaren data breach will require ongoing protections.

23. In addition, patients have spent substantial amounts of their time attempting to remedy the losses and securing their information and assets from further losses consequent to the breach.

IV. JURISDICTION AND VENUE

24. This action is brought as a class action under Michigan's Nonprofit Health Care Corporation Reform Act of 1980 (MCL 500.1406) and the Michigan Consumer Protection Act of 1976 (MCL 445.901, *et seq*.) and for common law negligence and breach of contract, and seeks monetary and equitable relief due to McLaren's unlawful, negligent, and unfair conduct.

25. This Court has personal jurisdiction over McLaren because McLaren does business within this judicial district and the claims asserted herein arise from conduct occurring, in part, within Michigan. This court also has original jurisdiction pursuant to 28 U.S.C. § 1332(d), as amended by the Class Action Fairness Act of 2005 ("CAFA").

26. Venue is proper in this Court because, *inter alia*, McLaren engages and performs business activities and is headquartered in this judicial district. Many of the acts committed by McLaren complained of herein occurred in this judicial district.

V. THE PARTIES

27. Plaintiff DAVID WEATHERS is, and at all relevant times was, a resident of the state of Michigan. Plaintiff WEATHERS was a patient at McLaren and he provided it with his PII, including his highly sensitive personal medical and financial information. He learned of the August 2023 data breach in October 2023 from media outlets. Plaintiff WEATHERS relied on and expected McLaren to take reasonable care with the information he provided McLaren so that he could use its services and, based on this reliance and expectation, allowed McLaren to access and hold his personal medical and financial information. As early as August 2023, and possibly sooner, McLaren negligently and illegally allowed a third-party access to Plaintiff WEATHERS's PII. Because of this negligent and illegal conduct, Plaintiff WEATHERS will incur substantial monetary and non-monetary losses, including the cost of mitigating the harm caused by the loss of privacy, the cost of identity theft protection and credit monitoring services, and stress, anxiety, and outrage associated with the release of his most personal information. Plaintiff WEATHERS has since spent hours of his own time attempting to research and remedy the loss and securing his assets and information.

28. Defendant McLaren Health Care Corporation is a 501(c)(3) corporation engaged in healthcare services, organized and existing under the laws of the State of Michigan, with its principal place of business located in Grand Blanc Michigan. It collects and maintains the personal medical information of individuals who submit to its facilities, which are primarily located in Michigan, but also collects and maintains such information from individuals who submit to testing and reside in other states. It operates, administers, and controls all of the McLaren entities' business activities, including the policies and procedures that led to the August 2023 breach.

VI. CLASS ALLEGATIONS

29. Plaintiff brings this action to seek monetary and equitable relief as a class action pursuant to Federal Rules of Civil Procedure, Rule 23, on behalf of himself and the following Class:

> All individuals whose personal information was released in the McLaren data breach disclosed in October 2023.

30. Plaintiff further brings this action on behalf of themselves and the following subclass (the "Michigan Subclass"):

> All Class members who were Michigan residents.

31. Plaintiff reserves the right to amend the Class or Subclass definitions if discovery or further investigation demonstrates that they should be expanded or otherwise modified.

32. The members of the Class are so numerous that joinder of all members would be impracticable. On information and belief, approximately 2,500,000 individuals' personal medical information was subject to unauthorized access, exfiltration, and theft.

33. There are questions of law and fact common to the members of the Class that predominate over any questions affecting only individual members, including:

a. Whether McLaren's sub-standard security protocols resulted in a breach of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of patients' sensitive personal medical information and to protect that information;

b. Whether McLaren's sub-standard security protocols resulted in a violation of an implied contractual obligation to safeguard the Class's sensitive personal medical information;

c. Whether McLaren's conduct violated Michigan's consumer protection and privacy laws; and

d. Whether, because of McLaren's misconduct, Plaintiff and the Class are entitled to compensatory damages, restitution, penalties, and equitable relief, and, if so, the amount and nature of such relief.

34. Plaintiff's claims are typical of the claims of the Class. Plaintiff has no interests antagonistic to those of the Class and is not subject to any unique defenses.

35. Plaintiff will fairly and adequately protect the interests of the Class and has retained attorneys experienced in class action and complex litigation.

36. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy for, *inter alia*, the following reasons:

a. It is economically impractical for members of the Class to prosecute individual actions;

b. The Class is readily ascertainable and definable;

c. Prosecution as a class action will eliminate the possibility of repetitious litigation; and

d. A class action will enable claims to be handled in an orderly and expeditious manner, will save time and expense, and will ensure uniformity of decisions.

37. Plaintiff does not anticipate any difficulty in the management of this litigation.

VII. CAUSES OF ACTION

First Cause of Action

(On Behalf of Plaintiff and the Michigan Subclass)

Violation of the Nonprofit Health Care Corporation Reform Act

(MCL 500.1406)

38. Plaintiff incorporates the above allegations as if set forth fully herein.

39. At all relevant times, Defendant was a "healthcare corporation" under the terms of MCL 500.1406 as an entity organized under sections 501(a) and 501(c) of the IRS Code and as a "nonprofit hospital service corporation," "medical care corporation," or a "consolidated hospital service," and defined by Michigan law.

40. At all relevant times, Plaintiff and the Michigan Subclass were "members" under the terms of MCL 500.1406 as subscribers, the dependents of subscribers, or other individuals entitled to receive health care benefits under a nongroup or group certificate under Michigan law.

41. By the acts described above, Defendant violated MCL 500.1406 by collecting, maintaining, and controlling its patients' sensitive personal medical information in a negligent and reckless manner and by designing, maintaining, and controlling systems that exposed its patients' sensitive personal medical information of which Defendant had control and possession to the risk of exposure to unauthorized persons, thereby violating its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. Defendant allowed unauthorized users to view, use, manipulate, exfiltrate, and steal the nonencrypted and nonredacted personal information of Plaintiff and other patients, including their personal medical information.

42. As a result of Defendant's violations, Plaintiff and the Michigan Subclass are entitled to all actual and compensatory damages according to proof or statutory damages allowable under MCL 500.1406, whichever are higher, to reasonable attorneys' fees and costs, and to such other and further relief as this Court may deem just and proper.

Second Cause of Action

(On Behalf of Plaintiff and the Michigan Subclass)

Violation of the Michigan Consumer Protection Act

(MCL 445.901, *et seq*., or "the MCPA")

43. Plaintiff incorporates the above allegations as if set forth fully herein.

44. Defendant is and at all relevant times was, subject to the provisions of the MCPA as an entity engaged in trade and commerce within the State of Michigan.

45. The acts and omissions described herein were undertaken in the course of Defendant's business of marketing, offering for sale, and selling goods and services.

46. Plaintiff and the Michigan Subclass are "consumers" as defined by the MCPA.

47. By the acts described above, Defendant violated the MCPA by engaging in unfair, unconscionable, and deceptive trade practices, as identified in MCL 445.903(1), including but not limited to:

(c) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has sponsorship, approval, status, affiliation, or connection that she or she does not have;

(e) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or mode, if they are of another;

(s) Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer; and

(cc) Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

48. Defendant made affirmative representations, including "pledges" and "commitments" to protect the security of Plaintiff's and Michigan Subclass members' PII, failed to implement measures to protect Plaintiff's and Michigan Subclass members' PII, failed to respond to affirmative warnings of security threats from the specific threat actors that executed the subject data breach, failed to identify foreseeable security risks and vulnerabilities in its network, failed to take reasonable steps to mitigate and defend against the threat posed by the threat actor, and failed to inform Plaintiff and Michigan Subclass members when the breach occurred in a timely manner.

49. Defendant omitted and actively concealed material facts regarding its inadequate security policies and practices from Plaintiff and the Michigan Subclass and withheld and continues to withhold information regarding the nature and quality of the August 2023 data breach. Had Defendant disclosed that its data systems lacked the almost universal safeguards described above, or had it disclosed that it had been warned of the likelihood that it would be targeted by a ransomware attack and refused or neglected to take the mitigating and defensive measures the state of Michigan had recommended, Plaintiff and the Michigan Subclass would not have allowed Defendant to collect and maintain their PII.

50. Defendant's acts and practices constitute a continuing and ongoing unfair business activity defined by the MCPA. Defendant's conduct is contrary to the public welfare as it transgresses civil statutes designed to protect individuals' constitutional and statutory right to

privacy, violates established public policy, and has been pursued to attain an unjustified monetary advantage for Defendant by creating personal disadvantage and hardship to its patients. As such, Defendant's business practices and acts have been immoral, unethical, oppressive and unscrupulous and has caused injury to customers far greater than any alleged countervailing benefit.

51. Defendant generated revenue by way of Plaintiff and the Michigan Subclass paying or generating medical insurance payments when entering transactions with Defendant where Defendant were the direct beneficiaries of these payments. Defendant's services were of lesser quality and value than Defendant represented in that Defendant did not take reasonable measures to safeguard customers' personal medical information. In reliance on Defendant's misrepresentations about its products and services, Plaintiff and the Michigan Subclass entered transactions with Defendant that they would not have, or for which Plaintiff and the Michigan Subclass would have paid less but for Defendant's representations.

52. Defendant's acts and omissions violated statutory and common law duties it owed to Plaintiff and the Class, including but not limited to duties to safeguard Plaintiff's and Michigan Subclass members' PII as required by HIPAA and MCL 500.1406.

53. As a direct and proximate consequence of the actions as identified above, Plaintiff and the Class suffered and continue to suffer harms and losses including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal medical information disclosed.

54. By engaging in the above-described unfair, unconscionable, and deceptive trade practices, Defendant committed and continues to commit one or more acts of unlawful and unfair conduct within the meaning of the MCPA. These acts and practices constitute a continuing and ongoing unlawful business activity defined by the MCPA, and justify the issuance of an injunction, restitution, and other equitable relief. Additionally, Plaintiff and the Michigan

Subclass members seek all actual and compensatory damages according to proof, reasonable attorneys' fees and costs, and to such other and further relief as this Court may deem just and proper.

Third Cause of Action

(On Behalf of Plaintiff and the Class)

Negligence

55. Plaintiff incorporates the above allegations as if set forth fully herein.

56. Defendant owed a duty of reasonable care to Plaintiff and the Class based upon Defendant's relationship to Plaintiff and the Class as a provider of medical services; based upon custom and practice in the healthcare industry; based upon Defendant's right to control information in its possession, exercise of control over the information in its possession, authority to control the information in its possession, and the commission of affirmative acts that resulted in the harms and losses alleged herein. Additionally, Defendant's duty is based on the requirements of MCL 500.1406 as a healthcare corporation operating in the State of Michigan.

57. Defendant breached its duty by collecting, maintaining, and controlling the Class's sensitive personal medical information in a negligent and reckless manner and by designing, maintaining, and controlling systems that exposed the Class's sensitive personal medical information, of which Defendant had control and possession, to the risk of exposure, and actual exposure, to unauthorized persons.

58. Defendant further committed *per se* breaches of duty by negligently violating the dictates of MCL 500.1406 by failing to safeguard the Class's sensitive personal medical information from unauthorized persons. The provisions of the Michigan Compiled Laws that Defendant violated were enacted to protect the class of persons involved here from the type of injury that occurred here, namely patients entitled to the right to privacy and the protection of their personal data.

59. As a direct consequence of the actions identified above, and the breaches of duties indicated thereby, unauthorized users gained access to, exfiltrated, stole, and gained disclosure of the sensitive personal medical information of Plaintiff and the Class, causing them harms and

losses including but not limited to the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, anxiety, stress, outrage, and privacy injuries associated with having their sensitive personal medical information disclosed.

Fourth Cause of Action

(On Behalf of Plaintiff and the Class)

Breach of Implied Contract

60. Plaintiff incorporates the above allegations as if set forth fully herein.

61. At all relevant times an implied contract existed and was in force between Defendant on one hand and Plaintiff and the Class on the other. This contract was implied by conduct and by written expressions Defendant maintained online.

62. The implied contract included promises and commitments made by Defendant, including but not limited to promises and commitments to safeguard the sensitive personal medical information Plaintiff and the Class entrusted to Defendant and to take reasonable action to expediently notify Plaintiff and the Class in the event of a breach of Defendant's systems that compromised the security of this information.

63. Plaintiff and the Class allowed Defendant to procure and maintain their personal medical information as a part of the provision of Defendant's services. Plaintiff and Class tendered money in exchange for Defendant's services and upon Defendant's solicitation or invitation. This exchange took place within the course of Defendant's regular business practices.

64. Defendant accepted Plaintiff and the Class's personal medical information for the purpose of providing services for Plaintiff and the Class, thereby entering an implied contract whereby Defendant became obligated to reasonably safeguard Plaintiff and the Class's personal medical information.

65. At the time Plaintiff and the Class supplied their personal medical information to and paid Defendant, Plaintiff and the Class intended to enter a relationship whereby and with the understanding that Defendant would adequately safeguard their personal medical information;

and ensure that others entrusted with the personal medical information would also protect the confidentiality of that information.

66. Plaintiff and the Class would not have entrusted their personal medical information to Defendant absent the existence of this implied contract. Had Defendant disclosed to Plaintiff and the Class that it lacked adequate security practices to safeguard personal medical information, Plaintiff and the Class would not have provided their personal medical information to Defendant.

67. Defendant knew or should have known by the nature of the information that personal medical information, such as medical records, are highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the Class.

68. At all relevant times and in all relevant ways, Plaintiff and the Class performed their obligations under the contract in question or were excused from performance of such obligations through the unknown and unforeseen conduct of others.

69. Defendant breached these duties and violated these promises by failing to properly safeguard the sensitive personal medical information of Plaintiff and the Class; by negligently and recklessly collecting, maintaining, and controlling this information; by designing, maintaining, and controlling systems that exposed its patients' sensitive personal medical information of which Defendant had control and possession to the risk of exposure to unauthorized persons; and by failing to inform Plaintiff and the Class in a reasonable time after the breach occurred.

70. As a direct consequence of the breaches of contract and violations of promises described above, unauthorized users gained access to, exfiltrated, stole, and gained disclosure of the sensitive personal medical information of Plaintiff and the Class, causing them harms and losses including but not limited to the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future expenses and time dedicated

to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal medical information disclosed.

VIII. PRAYER FOR RELIEF

Plaintiff, on behalf of himself and the Class, prays for relief and judgment against Defendant as follows:

1. For an order certifying the proposed Class and Subclass pursuant to Federal Rules of Civil Procedure, Rule 23;

2. For an order appointing Plaintiff and his counsel to represent the Class and Subclass;

3. For an order enjoining McLaren, its affiliates, successors, transferees, assignees, and the officers, directors, partners, agents, and employees thereof, and all other persons acting or claiming to act on its behalf or in concert with them, from continuing the unlawful practices as set forth herein, including but not limited to employing substandard data safety protocols to protect customer information, making ongoing false representations regarding the nature and quality of its data security, and from promising to fully compensate customer losses due to unauthorized use;

4. For actual and compensatory damages according to proof pursuant to Michigan law and all other applicable laws and regulations;

5. For restitution to the extent permitted by applicable law;

6. For civil and statutory penalties available under applicable law;

7. For pre-judgment and post-judgment interest;

8. For an award of attorneys' fees, costs, and expenses as authorized by applicable law; and

9. For such other and further relief as this Court may deem just and proper.

IX. DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the Class, demands a trial by jury on all issues so triable.

Respectfully submitted,

Dated this 16th day of October 2023.

/s/ David H. Fink

David H. Fink (P28235)
Nathan J. Fink (P75185)
FINK BRESSACK
38500 Woodward Ave., Suite 350
Bloomfield Hills, MI 48304
Telephone: (248) 971-2500
dfink@finkbressack.com
nfink@finkbressack.com

ERICKSON KRAMER OSBORNE, LLP
Julie C. Erickson*
Elizabeth A. Kramer*
Kevin M. Osborne*
44 Tehama St.
San Francisco, CA 94105
Telephone: (415) 635-0631
julie@eko.law
elizabeth@eko.law
kevin@eko.law

Attorneys for Plaintiff David Weathers

*Application for admission to be submitted