**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF MICHIGAN**

| | |
|---|---|
| JAMIE MCSKULIN, individually and on behalf of all others similarly situated,<br>Plaintiff,<br>v.<br>MCLAREN HEALTH CARE CORP.,<br>Defendant. | Case No.<br>CLASS ACTION<br>JURY TRIAL DEMANDED |

## CLASS ACTION COMPLAINT

Plaintiff Jamie McSkulin ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through undersigned counsel, brings this Class Action Complaint against Defendant McLaren Health Care Corporation ("McLaren"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

## INTRODUCTION

1. Plaintiff brings this class action against McLaren for its failure to secure and safeguard Plaintiff's and approximately 2.5 million patients and other individuals' ("Class members") private, confidential, and sensitive medical and personally identifying information ("PII/PHI"), including, upon information and belief: names, addresses, Social Security numbers, dates of birth, and medical and/or health insurance information (the "Data Breach").

2. Defendant is a $6.6 billion, fully integrated health care delivery system in Michigan that consists of 14 hospitals, ambulatory surgery centers, imaging centers, a 490-members employed primary and specialty care physician network, commercial and Medicaid HMOs

covering more than 732,838 residents in Michigan and Indiana, as well as Michigan's largest network of cancer centers.

3. Suspicious activity was initially detected in McLaren's IT systems in late August 2023, and it was eventually confirmed that it was a ransomware attack. On September 28, 2023, the Russian-linked ransomware group, BlackCat/AlphV, claimed responsibility for the attack and confirmed that the group exfiltrated more than 6 Terabytes of sensitive patient data from the McLaren's servers.

4. McLaren owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. McLaren breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their patients' PII/PHI from unauthorized access and disclosure.

5. As a result of McLaren's inadequate security measures and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all other individuals whose PII/PHI was exposed as a result of the Data Breach.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, breach of fiduciary duty, breach of implied contract, unjust enrichment, violations of the Michigan Consumer Protection Act, and violations of the Michigan data breach notification law, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

## PARTIES

***Plaintiff***

7. Plaintiff Jamie McSkulin is a Michigan resident who has paid for and received medical treatment and services numerous times at a McLaren medical facility. Believing McLaren would implement and maintain reasonable security practices to protect her PII/PHI, Ms. McSkulin routinely provided her PII/PHI to McLaren in connection with receiving medical treatment and services. She received three letters from McLaren in or around October 1, 2023 notifying her that her PII/PHI may have been exposed in the Data Breach. As a result of McLaren's conduct, Ms. McSkulin suffered actual damages including, without limitation, incurring time and expenses related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Ms. McSkulin will now be forced to expend additional time to review her credit reports and monitor her financial accounts and medical records for fraud or identity theft—particularly since the compromised information may include Social Security numbers and confidential medical information.

***Defendant***

8. Defendant McLaren Health Care. is a non-profit corporation organized under the state laws of Michigan with its principal place of business located at One McLaren Parkway, Grand Blanc, MI 48439.

## JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a

citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. This Court has personal jurisdiction over McLaren because McLaren is a corporation organized under the laws of Michigan.

11. Venue is proper pursuant to 28 U.S.C. § 1391(b)(2) because McLaren's principal place of business is located in this District.

## FACTUAL ALLEGATIONS

### *Overview of McLaren*

12. McLaren Health Care is a $6.6 billion health care system that operates 14 hospitals, ambulatory surgery centers, imaging centers, a 490-member employed primary and specialty care physician network, commercial and Medicaid HMOs covering more than 732,838 residents of Michigan and Indiana, home health, infusion and hospice providers, pharmacy services, a clinical laboratory network and a wholly owned medical malpractice insurance company. McLaren also operates Michigan's largest network of cancer centers and providers.[1]

13. To staff its extensive healthcare network, McLaren staffs 28,000 full-time, part-time, and contracted employees alongside more than 113,000 network providers throughout Michigan, Indiana, and Ohio.[2]

14. McLaren also offers a Graduate Medical Education program that maintains academic affiliations with medical schools at Wayne State University, Michigan State University, and Central Medical University.[3]

[1] *See* https://www.mclaren.org/main/about-mclaren-health-care (last accessed Oct. 5, 2023).
[2] *Id.*
[3] *Id.*

15. In the regular course of its business, McLaren collects and maintains the PII/PHI of individuals who participate in its health plan, patients, former patients, and other persons to whom it is currently providing or previously provided health-related services

16. McLaren requires patients to provide sensitive personal information before it provides treatment at its facilities and requires other individuals to provide information before being hired and participating in its health plan. Upon information and belief, that information includes, *inter alia*, names, addresses, dates of birth, health and health insurance information, and Social Security numbers. McLaren stores this information digitally.

17. McLaren's website contains a Web Privacy Policy, which states in pertinent part, "[t]he use and disclosure of the information you provide in such circumstances is governed by the Federal Health Insurance Portability And Accountability Act of 1996, more commonly known as HIPAA, as well as Michigan law."[4]

18. Additionally, McLaren's Notice of Privacy Practices, also available on its website, recognizes that[5]:

> We get information about you when you enroll in our health plans that is referred to as Protected Health Information or PHI. It includes your date of birth, gender, ID number, and other personal information. We also get bills and reports from your doctor and other data about your medical care which is also PHI . . . . We care about your privacy. The PHI we use and disclose is private . . . Only people who have both the need and legal right may see your PHI.

19. Plaintiff and Class members are, or were, patients of or otherwise affiliated with McLaren, participate in the McLaren health plan, and/or received health-related services from McLaren, and entrusted McLaren with their PII/PHI.

---

[4] *See* https://www.mclaren.org/main/web-privacy-policy (last accessed Oct. 5, 2023).
[5]https://www.mclarenhealthplan.org/uploads/public/documents/healthplan/documents/MHP%20Documents/NoticeofPrivacyPracticeMHP.pdf (last accessed Oct. 5, 2023)

20. Plaintiff and Class members, as former and current patients of or persons otherwise affiliated with McLaren, relied on these promises and on this well-established healthcare entity to keep their sensitive PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make certain only authorized disclosure of this information.

***The Data Breach***

21. In August 2023, McLaren detected suspicious activity in its IT systems.[6] McLaren did not disclose the date on which the unauthorized access first occurred or whether/when the unauthorized access concluded.

22. After an investigation, McLaren confirmed that it had experienced a ransomware attack that compromised the sensitive personal data of up to 2.5 million patients.[7]

23. In early September 2023, it was reported that McLaren's billing systems and electronic medical records were affected by the cybersecurity attack, and that workers at times had to use personal cellphones to communicate while the system was down.[8]

24. Then, on September 28, 2023, a notorious ransomware gang known as BlackCat/AlphV claimed responsibility for the attack on McLaren's systems, touting that "one of Michigan's largest healthcare companies was attacked by our group." The tweet went on to state

---

[6] Steve Adler, *McLaren Health Care Ransomware Attack May Affect Up to 2.5 Million Patients*, HIPAA JOURNAL. (Oct. 4, 2023), https://www.hipaajournal.com/mclaren-health-care-ransomware-attack-may-affect-up-to-2-5-million-patients/.

[7] Console & Associates, P.C., McLaren Health Care Targeted in Ransomware Attack That Hackers Claim Resulted in Data Breach Affecting 2.5 Million Patients, PR NEWSWIRE (Oct. 4, 2023), https://www.prnewswire.com/news-releases/console--associates-pc-mclaren-health-care-targeted-in-ransomware-attack-that-hackers-claim-resulted-in-data-breach-affecting-2-5-million-patients-301947820.html.

[8] Kristen Jordan Shamus, *McLaren Ransomware Attack May Have Leaked Patient Data to Dark Web*, DETROIT FREE PRESS (Oct. 4, 2023), https://www.freep.com/story/news/health/2023/10/04/mclaren-michigan-ransomware-attack-blackcat-alphv-dark-web-cybersecurity-breach-health/71056856007/.

that over 6 Terabytes of data was stolen from the company's servers.[9]

25. Terabytes ("TBs") are relatively large unites of digital data. To put it into perspective, it is estimated that 10 TBs could hold the entire printed collection of the U.S. Library of Congress, while a single TB could hold 1,000 copies of the Encyclopedia Brittanica.[10]

26. McLaren issued an update on the Data Breach stating that the healthcare network "immediately launched a comprehensive investigation to understand the source of the disruption and identify what, if any, data exposure occurred." The statement identifies that "[w]e are investigating reports that some of our data may be available on the dark web and will notify individuals whose information was impacted, if any, as soon as possible."[11]

27. Importantly, in direct response to BlackCat/AlphV's claim that "[o]ur backdoor is still running on your network," McLaren simply stated that it could not corroborate the claim at the time of their announcement.[12]

28. The ransomware group responsible for the Data Breach, BlackCat, is a criminal ring that has ties to Russia and was also implicated in a ransomware attack on a health system in Lehigh, Pennsylvania earlier this year.[13]

29. A spokesperson for McLaren said that its investigation is still ongoing as McLaren is in the process of reviewing the data that may have been compromised and will issue notifications to the affected individuals when that process has been completed. At this stage, McLaren has yet

---

[9] Vishwa Pandagle, *McLaren Healthcare: Largest Healthcare Data Breach by ALPHV, 6TB Data Stolen*, THE CYBER EXPRESS. (Sept. 29, 2023), https://thecyberexpress.com/alphv-blackcat-largest-healthcare-data-breach/.
[10] *See* https://www.teradata.com/Glossary/What-is-a-Terabyte (last accessed Oct. 5, 2023).
[11] *See McLaren Ransomware Attack May Have Leaked Patient Data to Dark Web, supra* n.8.
[12] *Id*.
[13] *Id*.

to confirm how many patients have been affected by the Data Breach.[14]

30. McLaren continues to withhold details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII/PHI remains protected. Without these details, Plaintiff's and Class members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

31. McLaren did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class members, causing the exposure of PII/PHI, such as encrypting the information or deleting it when it is no longer needed.

32. Upon information and belief, Plaintiff's and Class members' PII/PHI was compromised and acquired in the Data Breach.

33. As evidenced by the Data Breach's occurrence, the PII/PHI contained in McLaren's system was not adequately protected from intrusions. Had the information been properly secured consistent with industry standard and best practices, the data thieves would have exfiltrated only unintelligible data.

34. The ransomware group accessed and acquired files in McLaren's IT systems containing PII/PHI of Plaintiff and Class Members. Upon information and belief, such compromised information includes, *inter* alia, names, addresses, dates of birth, Social Security

[14] *See McLaren Health Care Ransomware Attack May Affect Up to 2.5 Million Patients, supra* n. 6.

numbers, and medical and treatment information. As a result, Plaintiff's and Class members' PII/PHI was accessed and stolen in the Data Breach, and their privacy has been jeopardized.

35. Plaintiff further believes that her PII/PHI, and that of Class members, was subsequently sold on the dark web following the Data Breach, as BlackCat/AlphV explicitly threatened to do so within "a few days of the attack,"[15] and that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

***McLaren Knew That Criminals Target PII/PHI***

36. At all relevant times, McLaren knew, or should have known, its patients', health plan participants', Plaintiff's, and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, McLaren failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that McLaren should have anticipated and guarded against.

37. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as Social Security numbers ("SSNs") and medical information—is valuable and frequently targeted by criminals. Indeed, "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[16]

38. In fact, the Data Breach is not McLaren's first experience with cybercriminals targeting the health network's extensive storage of patient information. In 2021, McLaren received notice of an earlier data security incident involving the network servers of its vendor Elekta AB

---

[15] *See McLaren Healthcare: Largest Healthcare Data Breach by ALPHV, 6TB Data Stolen, supra* n.9.

[16] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

that occurred between April 2 and April 20, 2021. The 2021 data incident compromised the following types of patient information: "full name, Social Security number, address, date of birth, height, weight, medical diagnosis, medical treatment details, appointment confirmations, and other information that McLaren Health Care Corporation may collect as a part of providing health care services."[17]

39. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.[18] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[19]

40. PII/PHI is a valuable property right.[20] The value of PII/PHI as a commodity is measurable.[21] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[22] American companies spend many billions of dollars on acquiring personal data of

---

[17] *See* https://www.mclaren.org/Uploads/Public/Documents/corporate/Elekta-Substitute-Notice.pdf (last accessed Oct. 5, 2023).

[18] Protenus, *2021 Breach Barometer*, PROTENUS.COM, available at https://www.protenus.com/resources/2021-breach-barometer (last accessed Oct. 5, 2023).

[19] Protenus, *2020 Breach Barometer*, PROTENUS.COM, available at https://www.protenus.com/resources/2020-breach-barometer (last accessed Oct. 5, 2023).

[20] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[21] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[22] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD LIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last accessed Oct. 5, 2023).

consumers.[23] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

41. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

42. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[24] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[25] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[26]

43. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each

---

[23] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last accessed Oct. 5, 2023) (estimated to have spent over $19 billion in 2018).

[24] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[25] *Id.*

[26] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

on the black market.[27] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[28]

44. John Riggi, the American Hospital Association National Advisor for Cybersecurity and Risk, said "foreign cyber gangs and spies" were testing the resilience of hospitals especially as hospitals began to fill up at the time because of the "tripledemic" including increased cases of RSV, flu and COVID-19.[29]

45. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[30] Quoting Carbon Black's Chief Cybersecurity Officer, one article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[31]

46. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies

---

[27] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last accessed Oct. 5, 2023).

[28] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last accessed Oct. 5, 2023).

[29] Dan Alexander, *Personal Data of 617,000 Patients Exposed in NJ Hospital Cyberattack*, NEW JERSEY 101.5 (Feb. 13, 2023), https://nj1015.com/personal-data-of-617000-patients-exposed-in-nj-hospital-cyberattack/.

[30] *What Happens to Stolen Healthcare Data*, *supra* at n. 23.

[31] *Id.*

confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[32]

47. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

***Theft of PII/PHI Has Grave and Lasting Consequences for Victims***

48. Theft of PII/PHI is serious. The Federal Trade Commission ("FTC") warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[33]

49. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[34] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card

---

[32] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

[33] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Oct. 5, 2023).

[34] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[35]

50. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits, or; filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[36]

51. Identity theft is a very difficult problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[37]

52. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[35] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[36] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Oct. 5, 2023).

[37] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Oct. 5, 2023).

53. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[38]

54. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[39] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[40] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[41] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[42]

55. For these reasons, the information compromised in the Data Breach is significantly more valuable than the loss of basic financial information, because there, victims can cancel or close credit or debit card accounts. Upon information and belief, the information compromised by

---

[38] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[39] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.

[40] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.27.

[41] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Oct. 5, 2023).

[42] *Id*.

the Data Breach—for example, a Social Security number—is exceedingly difficult, if not impossible, to change.

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

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[43]

57. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average, it takes

[43] *See The Geography of Medical Identity Theft*, *supra* at n.38.

approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[44]

58. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

***McLaren Fails to Comply With Industry Standards***

59. Cyber security experts routinely identify healthcare entities in possession of PII/PHI as being particularly vulnerable to cyberattacks because of the value of the information which they collect and maintain.

60. As a result, several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of PII/PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

61. McLaren failed to follow, enforce, or maintain the aforementioned best practices. McClaren also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3,

[44] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

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

***Damages Sustained by Plaintiff and the Other Class Members***

62. Plaintiff and Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

63. Plaintiff had a reasonable expectation of privacy in her sensitive PII/PHI while receiving medical services. Plaintiff would not have agreed to have her sensitive PII/PHI provided to and maintained by McLaren had she known that McLaren would fail to adequately protect their PII/PHI. Indeed, Plaintiff sought medical care through McLaren with the reasonable expectation that McLaren would keep her PII/PHI secure and inaccessible to unauthorized parties. Plaintiff and Class members would not have obtained services from McLaren had they known that McLaren failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII/PHI from criminal theft and misuse.

64. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to

compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

65. As a result of McLaren's failures, Plaintiff and Class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII/PHI. Indeed, Plaintiff's damages are not merely speculative. Consequently, Plaintiff and Class members now face a substantially increased risk of identity and medical theft that is plausibly imminent, considering the actual instances of fraud already suffered by other Class members.

## CLASS ALLEGATIONS

66. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

67. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

**Nationwide Class**

> All persons in the United States whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all persons who were sent a notice of the Data Breach.

68. Alternatively, Plaintiff seeks to certify this action on behalf of the following state class:

**Michigan Class**

> All persons in the state of Michigan whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all persons who were sent a notice of the Data Breach.

69. Excluded from the Class is McLaren Health Care Corporation and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

70. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

71. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

72. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. The ransomware group responsible for the Data Breach of McLaren's IT system represented that the stolen data includes the information of approximately 2.5 million patients.

73. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether McLaren had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether McLaren failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

c. Whether an implied contract existed between Class members and McLaren providing that McLaren would implement and maintain reasonable security

measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

d. Whether McLaren breached its duties to protect Plaintiff's and Class member's PII/PHI; and

e. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

74. McLaren engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

75. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by McLaren, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

76. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

77. 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 damages and other financial detriment suffered by Plaintiff

and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against McLaren, so it would be impracticable for Class members to individually seek redress from McLaren's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a 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 single adjudication, economy of scale, and comprehensive supervision by a single court.

## CAUSES OF ACTION

### COUNT I

### NEGLIGENCE

78. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

79. McLaren owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

80. McLaren knew the risks of collecting and storing Plaintiff's and Class members' PII/PHI and the importance of maintaining secure systems. McLaren knew of the many data breaches that targeted businesses that collect sensitive PII/PHI in recent years.

81. Given the nature of McLaren's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, McLaren should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

82. McLaren breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt,

implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

83. It was reasonably foreseeable to McLaren that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

84. But for McLaren's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

85. McLaren's duties also arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA 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 (collectively, "HIPAA Privacy and Security Rules").

86. McLaren's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as McLaren, of failing to employ reasonable measures to protect and secure PII/PHI.

87. McLaren violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and Class members' PII/PHI and not complying with applicable industry standards. McLaren's conduct was particularly unreasonable given the nature and amount of

PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

88. In addition, MCL § 550.1406, otherwise known as The Nonprofit Health Care Corporation Reform Act of 1980, requires that all medical facilities, such as those operated by McLaren, "ensure the confidentiality of records containing personal data that may be associated with identifiable members, use reasonable care to secure these records from unauthorized access." MCL § 550.1406(1).

89. McLaren violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. McLaren's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

90. In addition to its negligence, McLaren's violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

91. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

92. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the

same type of harm that has been suffered by Plaintiff and all other Class members as a result of the Data Breach.

93. It was reasonably foreseeable to McLaren that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

94. As a result of McLaren's above-described wrongful actions, inaction, and want of ordinary care, and its negligence and negligence per se, that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure, publication, and theft of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) the continued risk to their PII/PHI which remains in McLaren's possession; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face. In addition, Class members already have suffered actual fraud, identity theft, and medical theft as alleged herein, demonstrating how imminent the threat of such fraudulent activity and damages are to all Class members.

## COUNT II

## BREACH OF FIDUCIARY DUTY

95. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

96. Plaintiff and Class members provided McLaren their PII/PHI in confidence, believing that McLaren would protect that information. Plaintiff and Class members would not have provided McLaren with this information had they known it would not be adequately protected. McLaren's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between McLaren, on the one hand, and Plaintiff and Class members, on the other hand. In light of this relationship, McLaren must act primarily for the benefit of their patients and health plan participants, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

97. McLaren has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. McLaren breached that duty by failing to properly protect the integrity of their systems containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that they collected.

98. As a direct and proximate result of McLaren's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued

risk to their PII/PHI which remains in McLaren's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach. In addition, upon information and belief, Class members already have suffered actual fraud, identity theft, and medical theft, demonstrating how imminent the threat of such fraudulent activity and damages are to all Class members.

## COUNT III

## BREACH OF IMPLIED CONTRACT

99. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

100. In connection with receiving medical treatment, services, and/or participation in a health plan Plaintiff and Class members entered into implied contracts with McLaren.

101. Pursuant to these implied contracts, Plaintiff and Class members provided McLaren with their PII/PHI. In exchange, McLaren agreed to, among other things, among other things, and Plaintiff understood that McLaren would: (1) provide medical treatment, services, or health plan benefits to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

102. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and McLaren, on the other hand. Indeed, as set forth *supra*, McLaren recognized the importance of data security and the privacy of its patients' PII/PHI in, *inter alia*, its HIPAA Privacy Practices. Had Plaintiff and Class members known that McLaren

would not adequately protect their patients' and health plan participants' PII/PHI, they would not have participated in the health plan or received medical treatment or services from McLaren.

103. Plaintiff and Class members performed their obligations under the implied contract when they provided McLaren with their PII/PHI and paid—directly or through their insurers—for health care treatment, services, or health insurance premiums from Defendants.

104. McLaren breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

105. McLaren's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and Class members have suffered from the Data Breach.

106. Plaintiff and Class members were damaged by McLaren's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

## COUNT IV

## UNJUST ENRICHMENT

107. Plaintiff realleges and incorporate by reference all preceding paragraphs as if fully set forth herein.

108. This claim is pleaded in the alternative to the breach of implied contract claim.

109. Plaintiff and Class members conferred a monetary benefit upon McLaren in the form of monies paid for healthcare services or health insurance premiums.

110. McLaren accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. McLaren also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this information was used facilitate payment and make insurance claims.

111. As a result of McLaren's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff's and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

112. McLaren should not be permitted to retain the money belonging to Plaintiff and Class members because McLaren failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

113. McLaren should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

## COUNT V

### VIOLATIONS OF THE MICHIGAN CONSUMER PROTECTION ACT
### Mich. Comp. Laws §§ 455.901 *et seq*. ("MCPA")

114. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

115. Plaintiff and McLaren are "persons" under the MCPA. MCL § 455.902(d).

116. McLaren's transactions and conducting of business, namely providing employment, business process outsourcing, meetings and incentives, and exhibits and displays, with Plaintiff and Michigan Class members is "trade or commerce" under the MCPA. MCL § 455.902(g).

117. The MCPA lists 38 categories of practices that are considered unfair, unconscionable, or deceptive, and thus unlawful, under the statute. MCL § 455.903. Defendant's conduct in providing medical treatment, services, and/or participation in a health plan to Plaintiff and Class members while omitting or concealing that its data privacy practices are inadequate and that the sensitive information entrusted to it was exposed to a breach, constitutes unfair, unconscionable, deceptive, and thus unlawful, practices in at least the following categories:

a. "Representing that . . . services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have . . ." MCL § 455.903(c);

b. "Representing that . . . services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another" MCL § 455.903(e);

c. "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" MCL § 455.903(s); and

d. "Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner" MCL § 455.903(cc).

118. Had Plaintiff and Class members been aware of the omitted and misrepresented facts, i.e., that McLaren does not value data privacy and does not protect sensitive information, Plaintiff and the other Class members would not have sought medical services from McLaren.

119. Pursuant to MCL § 455.911(4), Plaintiff seeks damages on behalf of herself and Michigan Class members.

## COUNT VI

### VIOLATIONS OF MICHIGAN'S DATA BREACH NOTIFICATION STATUTE Mich. Comp. Laws §§ 445.71 *et seq*.

120. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

121. Plaintiff is authorized to bring this claim under MCL § 445.73(13).

122. McLaren is a corporation that owns, maintains, and records PII and PHI, and computerized data including PII and PHI, about its current and former patients, including Plaintiff and Class members.

123. McLaren is in possession of PII and PHI belonging to Plaintiff and Class members and is responsible for reasonably safeguarding that PII and PHI consistent with the requirements of MCL § 445.72.

124. McLaren failed to safeguard, maintain, and dispose of, as required, the PII/PHU within its possession, custody, or control, which it was required to do by Michigan law

125. McLaren knowingly and/or reasonably believing that Plaintiff's and Class members' PII and PHI was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members, as required by MCL § 445.72(1), (4).

126. As a result of McLaren's failure to reasonably safeguard Plaintiff's and Class members' PII/PHI, and the failure to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII/PHI in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

## PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against McLaren as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent McLaren from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: October 6, 2023

*/s/ Andrew W. Ferich*

Andrew W. Ferich
**AHDOOT & WOLFSON, PC**
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel: (310) 474-9111
Fax: (310) 474-8585
aferich@ahdootwolfson.com

Tina Wolfson
**AHDOOT & WOLFSON, PC**
2600 W. Olive Ave., Suite 500
Burbank, CA 91505-4521
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com