**UNITED STATES DISTRICT COURT**
**DISTRICT OF COLORADO**

| | | |
|---|---|---|
| PATRICIA DAVIDSON, individually and on behalf all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>HEALTHGRADES OPERATING COMPANY, INC.<br><br>Defendant. | ) | **CASE NO.**<br><br>**CLASS ACTION**<br><br>**JURY TRIAL DEMANDED** |

---

**CLASS ACTION COMPLAINT**

Plaintiff, Patricia Davidson, on behalf of herself and all others similarly situated, brings this action against Defendant HEALTHGRADES OPERATING COMPANY ("HOC" or "Defendant ") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from the Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

## I. NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") that was perpetrated against Defendant HOC, which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, "the Private Information") of the Plaintiff and the putative Class Members as a result of its contractual relationship with certain healthcare providers, including Wake Forest Baptist Health's Lexington Medical Center ("LMC"). As a result of the Data Breach, Plaintiff and thousands of

Class Members, suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.

3. The Private Information compromised in the Data Breach included names, addresses, demographic and contact information, Social Security numbers, dates of birth, medical record numbers, date(s) of service, patient type, health information, physician names, physician specialty, guarantor names, insurance types, insurance providers, and cost of treatment information.

4. The Private Information compromised in the Data Breach was exfiltrated by the cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect consumers' Private Information.

6. Plaintiff bring this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition

vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

9. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

10. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members'

names but with another person's photograph, and giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

16. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct.

## II. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

18. This Court has personal jurisdiction over Defendant because the conduct at issue in this case occurred, among other locations, in Colorado, where Defendant is headquartered.

19. Venue is proper because a substantial portion of the events complained of occurred in this District.

## III. PARTIES

20. Plaintiff Patricia Davidson is and at all times mentioned herein was as individual citizen of the State of North Carolina, residing in the city of Lexington. Plaintiff received notice of the Data Breach on or about March 26, 2021. A copy of the notice she received is attached hereto as Exhibit A (the "Notice Letter").

21. Defendant HOC is a Delaware corporation with its principal place of business at 1801 California Street, Suite 800, Denver, CO 80202, United States.

## IV. STATEMENT OF FACTS

### A. Nature of Defendant's Business.

22. Defendant is a US health technology company that provides information about physicians, hospitals and health care providers to consumers.

23. Defendant has amassed information on over 3 million U.S. health care providers.

24. According to USA Today, Defendant is the first comprehensive physician rating and comparison database.

25. Defendant provides information to consumers through a website and web application it operates that educates consumers on doctors' board certifications, types of procedures offered, and which insurance plans offices accept.

26. Defendant's website also lists a doctor's hospital affiliations and information on hospital performance collected from government data. Web visitors can input their opinions in a survey based on their experience with an individual health care professional, and view provider ratings at no charge. The survey evaluates a doctor's communication skills, the friendliness of the office staff, and whether it's easy to get an urgent appointment.

27. On information and belief, in the ordinary course of providing health care-focused services, Defendant also receives the Private Information of Plaintiff and Class Members from the various health care providers it rates and reviews, including LMC.

28. On information and belief, LMC contracted with HOC to provide IT support and educational services for its patients and community. Pursuant to that contractual relationship, Defendant HOC maintained personal information related to LMC's patients on its computer systems as a result of the services it provided to LMC.

29. Pursuant to the contract between LMC and HOC, LMC promised to, among other things, maintain and safeguard the personal information it received related to LMC's patients.

30. In the course of their contractual relationship, LMC provided HOC with at least the following Private Information of Plaintiff and Class Members:

a. name, address, phone number and email address;

b. dates of birth;

c. Social Security numbers;

d. information relating to individual medical history; and

e. medical record information.

31. LMC maintains, and is required to maintain, a HIPAA compliant Notice of Privacy Practices ("Privacy Policy").

32. The Privacy Policy posted on LMC's website is (upon information and belief) provided to each patient (including the Plaintiff here) prior to receiving treatment or services, and is provided to every patient upon request.[1]

33. The Privacy Policy states the following with respect to "business associates who perform functions on [LMC's] behalf" such as HOC:

> We may disclose protected health information to our business associates who perform functions on our behalf or provide us with services if the Protected Health Information is necessary for those functions or services. For example, we may use another company to do our billing, or to provide transcription or consulting services for us. **All of our business associates are obligated, under contract with us, to protect the privacy of your Protected Health Information.** [2]

34. Because of the highly sensitive and personal nature of the information LMC acquires and stores with respect to its patients, LMC promises: (1) "[e]nsure that health information that identifies you is kept private, except as such information is required or permitted to be disclosed by law;" (2) "[g]ive you this notice of our legal duties and privacy practices with respect to health information that [LMC] collect[s] and maintain[s] about you;" (3) to "not use or disclose your health information without your prior written authorization, except as permitted or required by law and described in this notice;" (4) to "abide by the terms of the Notice currently in effect," and; (5) "[a]fter learning of a breach…provide notice to you without unreasonable delay."[3]

---

[1] *See* https://www.lexmed.com/docs/privacy/Lexmed-privacypractices.pdf (last accessed April 26, 2021).
[2] *Id*. (emphasis added).
[3] *Id.*

35. LMC agreed to and undertook legal duties to maintain the protected health information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

36. Defendant HOC, acting as a business associate and vendor of LMC, held the patient information collected by LMC at its servers located in Denver, Colorado.[4]

37. The patient information held by LMC in its computer systems and networks included the Private Information of Plaintiff and Class Members.

**B. The Data Breach.**

38. On January 29, 2021 Defendant HOC notified LMC that an unauthorized individual gained access to one of its archived servers between October 16, 2020 and October 28, 2020.

39. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a healthcare technology company that collects, creates, and maintains both PII and PHI.

40. Because of this targeted cyberattack, data thieves were able to gain access to files that included patient information from the time HOC provided services to LMC.

41. The archived server and files contained therein affected by this incident contained the following information of Plaintiff and Class Members: names, addresses, demographic and contact information, Social Security numbers, dates of birth, medical record numbers, date(s) of service, patient type, health information, physician names, physician specialty, guarantor names, insurance types, insurance providers, and cost of treatment information.

---

[4] *See* Notice Letter.

42. The Private Information contained in the emails was not encrypted.

43. Plaintiff's Private Information was accessed and stolen in the Data Breach. Plaintiff further believes her stolen Private Information was subsequently sold on the Dark Web.

44. Unsurprisingly, it could not be ruled out that Private Information was viewed or accessed in the Data Breach.[5]

45. LMC informed its patients, including Plaintiff and Class Members, that they should enroll in identity monitoring services as well as take additional steps in response to the Data Breach.[6]

46. That LMC is encouraging its patients to enroll in identity monitoring services is an acknowledgment that the impacted customers are subject to an imminent threat of fraud and identity theft.

47. Despite discovering the Data Breach on or about January 29, 2021, HOC still has not notified any affected persons.[7] Plaintiff only learned of this breach through LMC.

48. HOC had obligations created by HIPAA, contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

49. HOC's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

---

[5] *See* Exhibit A attached hereto.
[6] *Id.*
[7] *Id*.

50. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), HOC knew or should have known that its electronic records would be targeted by cybercriminals.

51. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets, such as healthcare companies like HOC, so they are aware of, and prepared for, a potential attack.[8]

52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in HOC's industry, including Defendant.

***Defendant Fails to Comply with FTC Guidelines***

53. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In 2016, the FTC updated its publication, *Protecting Personal Information: A*

---

[8] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Jan. 13, 2021).

*Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[9] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

---

[9] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 14, 2021).
[10] *Id*.

to meet their data security obligations.

57. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

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

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

60. Defendant was at all times fully aware of its obligation to protect the PII and PHI of Plaintiff and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

***Defendant Fails to Comply with Industry Standards***

61. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

62. Several best practices have been identified that a minimum should be implemented by healthcare providers 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.

63. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards.

64. The Center for Internet Security (CIS) released its *Critical Security Controls*, and all healthcare institutions are strongly advised to follow these actions. The CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[11]

65. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

66. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; General Accounting Office (GAO) standards; the Federal Risk and Authorization Management Program (FEDRAMP); and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

***Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security***

67. HIPAA requires covered entities to protect against reasonably anticipated threats

---

[11] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan. 14, 2021).

to the security of sensitive patient health information.

68. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

69. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data HOC left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

70. HOC's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

## DEFENDANT'S BREACH

71. HOC breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. HOC's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing PII and PHI;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

p. Failing to adhere to industry standards for cybersecurity.

72. As the result of computer systems in dire need of security upgrading, HOC negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

73. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain LMC made with HOC, of which they were third-party beneficiaries.

***Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft***

74. Cyberattacks and data breaches like the one at HOC are especially problematic because of the disruption they cause to the overall daily lives of patients affected by the attack.

75. The United States Government Accountability Office released a report in 2007

regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

76. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

77. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent

---

[12] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[13]

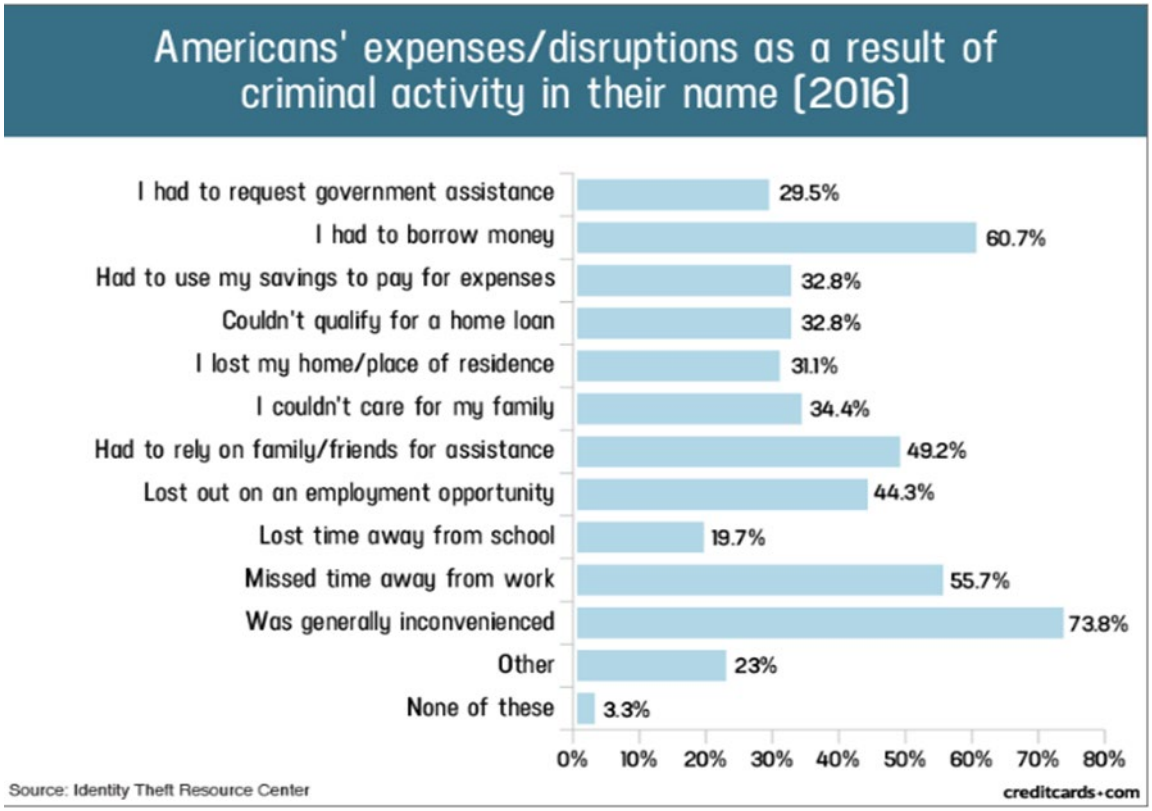
78. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

79. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, 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.

80. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[14]

---

[13] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited January 13, 2021).
[14] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.




81. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[15]

82. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

83. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or

---

[15] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[16]

84. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

85. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

86. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

*See* GAO Report, at p. 29.

87. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-

---

[16] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 13, 2021).

market" for years.

88. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

89. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

90. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[17] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

91. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[18] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[19] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an

---

[17] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[18] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 14, 2021).
[19] *Id* at 4.

individual's authentic tax return is rejected.

92. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

93. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

94. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[21]

95. Medical information is especially valuable to identity thieves.

96. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[22] That pales in comparison with the asking price for medical data, which was selling for $50 and

---

[20] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[22] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

up.[23]

97. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

98. For this reason, HOC knew or should have known about these dangers and strengthened its computer systems accordingly. HOC was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

***Plaintiff's and Class Members' Damages***

99. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

100. Defendant is not even offering the standard 12 months of complimentary fraud and identity monitoring services typically offered in data breaches. This is utterly unacceptable as it leaves numerous victims of the breach vulnerable to all sorts of fraud and identity theft.

101. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

102. Plaintiff has expended a great deal of time and effort dealing with Defendant's Data Breach.

103. As a result of the Data Breach, Plaintiff has experienced an increase in the amount of suspicious and unsolicited phishing phone calls, texts and emails she receives, all of which appear to be placed with the intent to obtain personal information to commit identity theft by way

---

[23] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

of a social engineering attack.

104. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports, medical insurance claims, and financial accounts for any indications of actual or attempted identity theft or fraud. Plaintiff now spends approximately 1.5 hours per week reviewing her credit monitoring reports and sensitive medical and financial accounts for irregularities. Since being notified of the Data Breach, Plaintiff has spent at least 7.5 hours on these tasks, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

105. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff is very upset that her Private Information is in the hands of data thieves. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

106. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff will continue to be at increased risk of identity theft and fraud for years to come.

107. Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

108. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

109. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

110. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

111. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

112. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

113. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

114. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to LMC was intended to be used by Defendant to fund adequate security of Mercy's computer property and

protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

115. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

116. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges, insurance claims, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

113. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such

data is properly encrypted.

114. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

115. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

## V. CLASS ACTION ALLEGATIONS

116. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

117. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons who utilized LMC and whose Private Information was maintained on Defendant HOC's computer systems that were compromised in the Data Breach, and who were sent Notice of the Data Breach by LMC.

118. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

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

120. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of persons whose data was compromised in Data Breach.

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant's acts, inactions, and practices complained of herein violated the Colorado data protection laws invoked below;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

122. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

123. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

124. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common

issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

125. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

126. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

127. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

128. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by LMC.

## CAUSES OF ACTION

### FIRST COUNT
### Negligence
### (On behalf of Plaintiff and All Class Members)

129. Plaintiff re-alleges and incorporate by reference Paragraphs 1 through 128 above as if fully set forth herein.

130. LMC required Plaintiff and Class Members to submit non-public personal information in order to obtain medical services, and then in turn disclosed or otherwise turned over this non-public personal information to Defendant HOC.

131. Pursuant to its contract with LMC referenced above, Defendant HOC agreed to and assumed a duty to safeguard the privacy and security of any PII or PHI that LMC shared with it.

132. Through its relationship as a business associate or vendor of LMC's, Defendant HOC agreed to and undertook legal duties to maintain the protected health information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws, including HIPAA.

133. By accepting PHI for storage, Defendant HOC became a "covered entity" under HIPPA, and undertook legal duties to maintain the protected health information entrusted to it safely, confidentially, and in compliance with all applicable laws, including HIPAA.

134. By storing this data in its computer property, and using it for commercial gain, Defendant HOC had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants HOC's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

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

136. Defendant HOC owed a duty of care to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53,

53A, or 800-171; General Accounting Office ("GAO") standards; the Federal Risk and Authorization Management Program ("FEDRAMP"); and the Center for Internet Security's Critical Security Controls ("CIS CSC"), which are all established industry standards in reasonable cybersecurity readiness.

137. Defendant HOC owed a duty of care to Plaintiff and Class Members to provide data security consistent with applicable standards of care from statutory authority like HIPPA and Section 5 of the FTCA, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

138. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

139. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

140. Plaintiff and Class Members are within the class of persons that the HIPAA was intended to protect.

141. The harm that occurred as a result of the Data Breach is the type of harm that HIPAA was intended to guard against. The Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures relating to protected health information, caused the same harm as that suffered by Plaintiff and the Class.

142. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

143. Defendant HOC was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

144. Defendant HOC knew or should have known that its own data security systems posed a foreseeable risk of compromise, based upon the explosion of data breaches involving the financial services and medical care industries detailed above.

145. Defendant HOC's duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

146. In addition, Defendant HOC had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

147. Defendant HOC's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants is bound by industry standards to protect confidential Private Information.

148. Defendant HOC breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to implement multifactor authentication;

e. Failing to apply all available security updates;

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

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

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

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

j. Failing to properly train and supervise employees in the proper handling of inbound emails;

k. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

l. Failing to adequately monitor the security of its networks and systems;

m. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

n. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;

o. Failing to meet industry standards for cybersecurity readiness;

p. Failing to detect in a timely manner that Plaintiffs' and Class Members' Private Information had been compromised, and;

q. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

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

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

151. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

152. Defendant HOC's negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner, and b) have not reported securing its servers that were breached in the Data Breach. Plaintiff and Class Members

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

**SECOND COUNT**
**Invasion of Privacy by Intrusion**
**(On Behalf of Plaintiff and All Class Members)**

153. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 128 as if fully set forth herein.

154. The State of Colorado recognizes the tort of Invasion of Privacy by Intrusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

155. Plaintiff and the Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

156. By intentionally failing to keep Plaintiff's and the Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by intrusion.

157. Defendant knew that ordinary persons in Plaintiff's or the Class Members' positions would consider this an invasion of privacy and Defendant's intentional actions highly offensive and objectionable.

158. Defendant invaded Plaintiff's and the Class Members' right to privacy and intruded into Plaintiff's and the Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

159. Defendant intentionally concealed from Plaintiff and the Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

160. In failing to protect Plaintiff's and the Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and the Class Members' rights to have such information kept confidential and private.

161. Plaintiff and the Class Members sustained damages (as outline above) as a direct and proximate consequence of the invasion of their privacy by intrusion, and therefore seek an award of damages.

**THIRD COUNT**
**Violation of Colorado's Data Security Laws, Colo. Rev. Stat. § 6-1-713.5**
**(On Behalf of Plaintiff and All Class Members)**

162. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 128 above as if fully set forth herein.

163. Plaintiff brings this claim on behalf of herself and the Class.

164. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

165. Colo. Rev. Stat. § 6-1-713.5 requires commercial entities who maintain, own, or license "personal identifying information of an individual residing in the state" to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

166. Defendant's conduct violated Colo. Rev. Stat. § 6-1-713.5. Specifically, Defendant voluntarily undertook the act of maintaining and storing Plaintiff's PII and PHI but Defendant failed to implement safety and security procedures and practices sufficient enough to protect from the data breach that it should have anticipated. Defendant should have known and anticipated that data breaches—especially health data—were on the rise, and that medical institutions were lucrative or likely targets of cybercriminals looking to steal PII. Correspondingly, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

167. As a result of Defendant's violation of Colo. Rev. Stat. § 6-1-716, Plaintiff and the Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

168. Accordingly, Plaintiff, individually and on behalf of the Class, respectfully request this Court award all relevant damages.

**FOURTH COUNT**
**Violation of Colorado's Security Breach Notification Laws, Colo. Rev. Stat. § 6-1-716**
**(On Behalf of Plaintiff and All Class Members)**

169. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 128 above

as if fully set forth herein.

170. Plaintiff brings this claim on behalf of herself and the Class.

171. Defendant's conduct violated Colo. Rev. Stat. § 6-1-716, which requires commercial entities to notify individuals within 30 days of a security that involves personal information.

172. The Data Breach occurred in October of 2020. Defendant claims it did not discover the breach until January 29, 2021. However, Defendant still has not given notice of the breach to Plaintiff and the Class Members.

173. Defendant unreasonably delayed informing anyone about the breach of security of Plaintiff's and the Class Members' confidential and non-public information after Defendant knew the Data Breach had occurred.

174. Defendant failed to disclose to Plaintiff or the Class Members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted—or not properly and securely encrypted—PII and PHI when it knew or reasonably believed such information had been compromised.

175. As a result of Defendant's violation of Colo. Rev. Stat. § 6-1-716, Plaintiff and the Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

176. Accordingly, Plaintiff, individually and on behalf of the Class, respectfully requests this Court award all relevant damages.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

b. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants ' wrongful conduct;

e. Ordering Defendants to pay for not less than seven years of credit monitoring services for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

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

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury on all claims so triable.

Dated: May 6, 2021

Respectfully submitted,

/s/ *Gary M. Klinger*
Gary M. Klinger
**MASON LIETZ & KLINGER LLP**
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (202) 429-2290
Email: gklinger@masonllp.com

Gary E. Mason*
David K. Lietz*
**MASON LIETZ & KLINGER LLP**
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dlietz@masonllp.com

**pro hac vice to be filed*

*Attorneys for Plaintiff*

# EXHIBIT A

Lexington Medical Center

March 26, 2021

79 1 20504 **********AUTO**5-DIGIT 27295
PATRICIA B DAVIDSON
[redacted]
LEXINGTON, NC [redacted]

**Su información personal puede haber estado involucrada en un posible incidente cibernético. Si desea recibir una versión de esta carta en español, por favor llame 1-855-660-1531.**

Dear Patricia B Davidson,

Lexington Medical Center (LMC) (formerly known as Lexington Memorial Hospital) is proud to provide quality healthcare for our community, and we are honored by the trust you and others place in us to care for you. We recognize an important part of that trust includes protecting the privacy and security of your information, including when that information is maintained by our vendors. Unfortunately, we have discovered that Healthgrades Operating Company, Inc. ("Healthgrades"), a vendor who previously provided services to LMC, has had a security incident that involved some of your information.

**What Happened?**

Healthgrades previously assisted LMC in educating patients and the community about health matters and available services at LMC. In order to provide those services, Healthgrades was provided some LMC information. On January 29, 2021, Healthgrades notified us that an unauthorized individual gained access to a Healthgrades archived server between October 16, 2020 and October 28, 2020. Healthgrades discovered that the impacted archived server included backup files with LMC patient information from the time it provided services to LMC. The files included information from mid-2010 to mid-2011.

**What Information Was Involved?**

As soon as we were notified by Healthgrades, we immediately took steps to understand the circumstances of the incident and the information impacted. We understand that the Healthgrades files involved in the incident were archived files maintained by Healthgrades from the time when they provided services to LMC. The information in the files did not include your financial account information. In addition, because LMC is no longer using Healthgrades to provide these services, the files did not include information from any recent services.

The archived files may have included your name, address, demographic and contact information, Social Security number, date of birth, LMC medical record number, date(s) of service, patient type, limited health information such as treatment and billing codes and their descriptions (which, in some cases, may indicate a diagnosis), physician names, physician specialty, guarantor name, insurance type, insurance provider, and/or cost of treatment information. This incident was limited to the Healthgrades systems only and did **not** involve any LMC systems or electronic health records.

**What Are We Doing in Response?**

We care about the privacy and security of our patients' information and take this matter very seriously. To help prevent something like this from happening again, we have obtained assurances from Healthgrades that no LMC patient data remains on their systems. LMC has similarly reviewed its files and confirmed that no patient information is being sent to Healthgrades. Finally, Healthgrades has also advised us that they have notified law enforcement of this incident and will cooperate with any follow up investigation.

**What Can You Do?**

Although we have received no indication that your information has been misused, out of an abundance of caution, we are offering you complimentary identity monitoring services through Kroll for one year. The services being offered

include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. We also recommend you review the statements you receive from your healthcare providers. If you see services you did not receive, please contact the provider immediately. **For more information about the identity monitoring services, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the pages that follow this letter.**

**For More Information**

We are very sorry for any concern or inconvenience this incident may cause you. If you have questions, please contact 1-855-660-1531, Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time.

Sincerely,

Patricia Corn
Chief Privacy Officer