IN THE IOWA DISTRICT COURT FOR MARSHALL COUNTY

ROBERT MYSHKA and DANIEL STUMME, individually and on behalf of all others similarly situated, Plaintiffs, v. WOLFE CLINIC, P.C. d/b/a WOLFE EYE CLINIC, Defendant.	Case No. _____ **CLASS ACTION PETITION and JURY TRIAL DEMANDED**

CLASS ACTION PETITION

Plaintiffs ROBERT MYSHKA and DANIEL STUMME ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this class action lawsuit against Defendant Wolfe Clinic, P.C. ("Wolfe" or "Defendant"), an Iowa professional corporation that does business as "Wolfe Eye Clinic," to obtain damages, restitution and injunctive relief for the Classes, as defined below. Plaintiffs make the following allegations upon information and belief, except as to his own actions, the investigation of his counsel and certain facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action lawsuit arises out of the *recently* announced targeted ransomware cyberattack and data breach (the "Data Breach") that occurred at Wolfe, a specialty medical eye care and surgical treatment center with locations across the State of Iowa.

2. As a result of the Data Breach, Plaintiffs and approximately 500,000 current and former patients of Wolfe (nearly all of whom are residents of Iowa) 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.

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

4. Information compromised in the Data Breach includes patient names, dates of birth, Social Security numbers, health insurance information and medical treatment information and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively, the "Private Information").

5. Plaintiffs bring this class action lawsuit to address Wolfe's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and 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.

6. 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, such as the one that occurred in early February of this year thereby enabling access to Defendant's network and, ultimately, to the Private Information.

7. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus it 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. 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 been able to prevent or, at least, to discover the intrusion sooner, been able to complete its investigation and notify affected persons much earlier than June 22, 2021, *135 days after the Data Breach*.

9. Plaintiffs' 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.

10. 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' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and/or giving false information to police during an arrest.

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

12. Plaintiffs 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 to detect identity theft.

13. Plaintiffs seek to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs and injunctive relief including improvements to Wolfe's data security systems, future annual audits and adequate credit monitoring services (beyond twelve months) funded by Defendant.

PARTIES

15. Plaintiff ROBERT MYSHKA is, and at all times mentioned herein was, an individual citizen of the State of Iowa residing in the City of Waterloo. Plaintiff was notified of Defendant's Data Breach and his Private Information being compromised upon receiving a letter titled "Notice of a Data Breach" and dated as of June 29, 2021.

16. Plaintiff Daniel Stumme is, and at all times mentioned herein was, an individual citizen of the State of Iowa residing in the City of Waterloo. Plaintiff was notified of Defendant's Data Breach and his Private Information being compromised upon receiving a letter titled "Notice of a Data Breach" and dated as of June 29, 2021.

17. Defendant Wolfe, a specialty medical eye care and surgical treatment center with locations across the State of Iowa, maintains its corporate offices at 309 East Church Street in Marshalltown, Iowa 50158.

JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over Plaintiffs' claims under Iowa Code § 602.6101.

19. Venue is proper in Marshall County pursuant to Iowa Code § 616.17 and § 616.18 because Defendant Wolfe is headquartered and does business in this County, the cause of action

accrued in this county and Wolfe has an office for the transaction of its customary business in this county.

20. The Court has personal jurisdiction over Defendant because it is an Iowa professional corporation with its principal place of business in Iowa, committed tortious acts in Iowa and because it has sufficient minimum contacts and has engaged in significant business activity in the State of Iowa.

DEFENDANT'S BUSINESS

21. Defendant Wolfe, founded in 1919 in Marshalltown, Iowa, is a specialty medical eye care and surgical treatment center with locations across the State of Iowa.

22. According to its website, Wolfe owns and operates eleven clinics in Iowa, as well as nine family vision centers, a state-of-the art surgical center and more than twenty-five outreach locations.[1]

23. In the ordinary course of receiving treatment and health care services from Wolfe, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Financial account information;
- Payment card information;
- Medical histories;
- Treatment information;

[1] https://www.wolfeeyeclinic.com/about (last visited June 29, 2021).

- Medication or prescription information;
- Provider information;
- Address, phone number and email address and
- Health insurance information.

24. Additionally, Wolfe may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends and/or family members.

25. Due to the highly sensitive and personal nature of the information it acquires and stores with respect to its patients, Wolfe proclaims that it takes the "security of all information in our control very seriously."[2]

26. Specifically, Wolfe, in its privacy policy, states

> We understand that medical information about you and your health is personal. Protecting medical information about you is important. We create a record of the care and services you receive.[3]

27. Thus, as disclosed in its Privacy Policy, Wolfe promises to maintain the confidentiality of patients' health, financial and non-public personal information, ensure compliance with federal and state laws and regulations and to notify patients of any breach that jeopardizes their private information:

> We are required by law to maintain the privacy of protected health information and to give you this Notice explaining our privacy practices with regard to that information. You have certain rights and we have certain legal obligations regarding the privacy of your protected health information. This Notice explains your rights and

---

[2] https://www.wolfeeyeclinic.com/alert-info?id=b900ea23-c911-4a89-b323-c0d9ef005bb0 (last visited June 29, 2021).

[3] https://www.wolfeeyeclinic.com/privacy-policy (last visited June 29, 2021).

> our obligations. We are required to abide by the terms of the current version of this Notice.[4]

28. As a condition of receiving medical care and treatment at one of Defendant's facilities, Wolfe requires that its patients entrust it with highly sensitive personal information.

29. By obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' Private Information, Wolfe assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized access and/or disclosure.

30. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

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

THE CYBERATTACK AND DATA BREACH

32. Not until June 22, 2021, did Wolfe announce that it was the victim of a ransomware attack on or about February 8, 2021.

33. According to Wolfe's "Notice of Data Incident," as well as certain media reports, hackers gained access to its systems and used ransomware to encrypt files.

34. According to those reports, a ransom demand was issued for the keys to decrypt files, but the clinic refused to pay and opted to recover files from backups. The attackers were thus able to exfiltrate records of approximately 500,000 affected persons from Wolfe Eye Clinic

[4] https://www.wolfeeyeclinic.com/privacy-policy (last visited June 29, 2021).

systems.[5]

35. Despite the occurrence of the attach in early February, Wolfe did not get a grasp of the full scale of the records compromised until late May; indeed, according to Wolfe, "[d]ue to the scale and complexity of the attack, it took until May 28, 2021 for the full scope of the security breach to be determined and to identify the information compromised in the attack."[6]

36. Even then, although the "full scope of the security breach" was known as of May 28, 2021 and the "forensic investigation [had] concluded on June 8, 2021," Wolfe nonetheless did not begin to notify affected individuals until June 22, 2021.[7]

37. In fact, Plaintiffs' Notice was not sent until June 29, 2021. *See* Exhibit 1.

38. The stolen protected health information included names, addresses, birth dates, Social Security numbers and, for some individuals, medical and health information.

39. The attackers appear to have exfiltrated a large amount of data. *KCCI Des Moines* has reported the incident as affecting approximately 500,000 individuals, making this one of the most extensive ransomware attacks on a single healthcare provider to have been reported this year.[8]

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

---

[5] https://www.hipaajournal.com/phi-of-up-to-500000-individuals-potentially-stolen-in-wolfe-eye-clinic-ransomware-attack/ (last visited June 29, 2021).

[6] https://www.wolfeeyeclinic.com/alert-info?id=b900ea23-c911-4a89-b323-c0d9ef005bb0 (last visited June 29, 2021).

[7] *Id.*

[8] https://www.kcci.com/article/wolfe-eye-clinic-cyberattack-reported/36806166 (last visited June 29, 2021).

41. Upon information and belief, the targeted cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiffs and the Class Members.

42. Because of this cyberattack, data thieves were able to gain access to and exfiltrate the protected Private Information of hundreds of thousands of Wolfe patients.

43. Plaintiffs' Private Information was accessed and stolen in the Data Breach. Plaintiffs further believe their stolen Private Information was subsequently sold on the Dark Web.

44. Beginning on June 22, 2021, Wolfe informed impacted customers that they should take steps to protect themselves against fraudulent activity and identity theft and to remain vigilant about unauthorized access to their accounts.[9]

45. Further, though Wolfe impliedly acknowledges that its system was inadequate to prevent such a cyberattack (and thereby protect the confidential Private Information it swore to protect),[10] Defendant is only offering a complimentary twelve month membership of identity monitoring services for victim patients.[11]

46. The offer of identity monitoring services is an acknowledgment by Wolfe that the impacted customers are subject to an imminent threat of fraud and identity theft.

47. Despite discovering the Data Breach on or about February 8, 2021, and acknowledging that data thieves likely accessed Plaintiffs' and the Class Members' Private

---

[9] https://www.wolfeeyeclinic.com/alert-info?id=b900ea23-c911-4a89-b323-c0d9ef005bb0 (last visited June 29, 2021).

[10] *Id.* (stating that "[w]e are taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in our systems.").

[11] *Id.*

Information, Wolfe took months to complete its investigation and even then took additional weeks to begin to notify affected patients on June 22, 2021, 135 days after the initial discovery of the Data Breach.[12]

48. Wolfe had obligations created by HIPAA, contract, industry standards, common law as well as its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

49. Plaintiffs and Class Members provided their Private Information to Wolfe with the reasonable expectation and mutual understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized access.

50. Wolfe'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.

51. 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), Wolfe knew or should have known that its electronic records would be targeted by cybercriminals.

---

12 *Id*.

52. In fact, in 2021 alone there have been over 220 data breach incidents.[13] These approximately 220 data breach incidents have impacted nearly 15 million individuals.[14]

53. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and the United States Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[15]

54. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[16]

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

Defendant Fails to Comply with FTC Guidelines

56. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

57. According to the FTC, the need for data security should be factored into all business decision-making.

---

[13] *See* Kim Delmonico, Another (!) Orthopedic Practice Reports Data Breach, Orthopedics This Week (May 24, 2021), https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/ (last visited July 6, 2021).

[14] *Id*.

[15] *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 July 6, 2021).

[16] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited July 6, 2021).

58. In 2016, the FTC updated its publication, *Protecting Personal Information: A 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.[17]

59. 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.[18]

60. 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.

61. 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

---

[17] *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 July 6, 2021).

[18] *Id.*

to meet their data security obligations.

62. 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.")

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

64. 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.

65. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients.[19] Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

66. As noted 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.

67. 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;

[19] *See* https://www.wolfeeyeclinic.com/privacy-policy ("We are required by law to maintain the privacy of protected health information and to give you this Notice explaining our privacy practices with regard to that information.").

encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

68. 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.

69. 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.[20]

70. 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.

71. Defendant 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, 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.

72. These foregoing frameworks are existing and applicable industry standards in the

[20] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited July 6, 2021).

healthcare industry, and in the healthcare administrative services industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

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

73. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

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

75. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*.

76. 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 Wolfe 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).

77. Ransomware attacks are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."[21]

[21] *See* 45 C.F.R. 164.40.

78. Wolfe's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

79. Wolfe breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data.

80. Wolfe'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, ransomware 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 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);

f. 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);

g. 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);

h. 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);

i. 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);

j. 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);

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

l. 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);

m. 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");

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

o. Failing to adhere to industry standards for cybersecurity.

81. As the result of, among other things, maintaining computer systems in dire need of security upgrading, *see* Notice of Data Incident, Wolfe negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

82. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Wolfe.

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

83. Cyberattacks and data breaches at healthcare providers like Wolfe are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

84. 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."[22]

85. 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.

86. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and to 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

[22] *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 (last visited July 6, 2021).

it is for the thief to take on the victim's identity or otherwise harass or track the victim.

87. 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.

88. 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 charges from their accounts, placing a credit freeze on their credit and correcting their credit reports.[23]

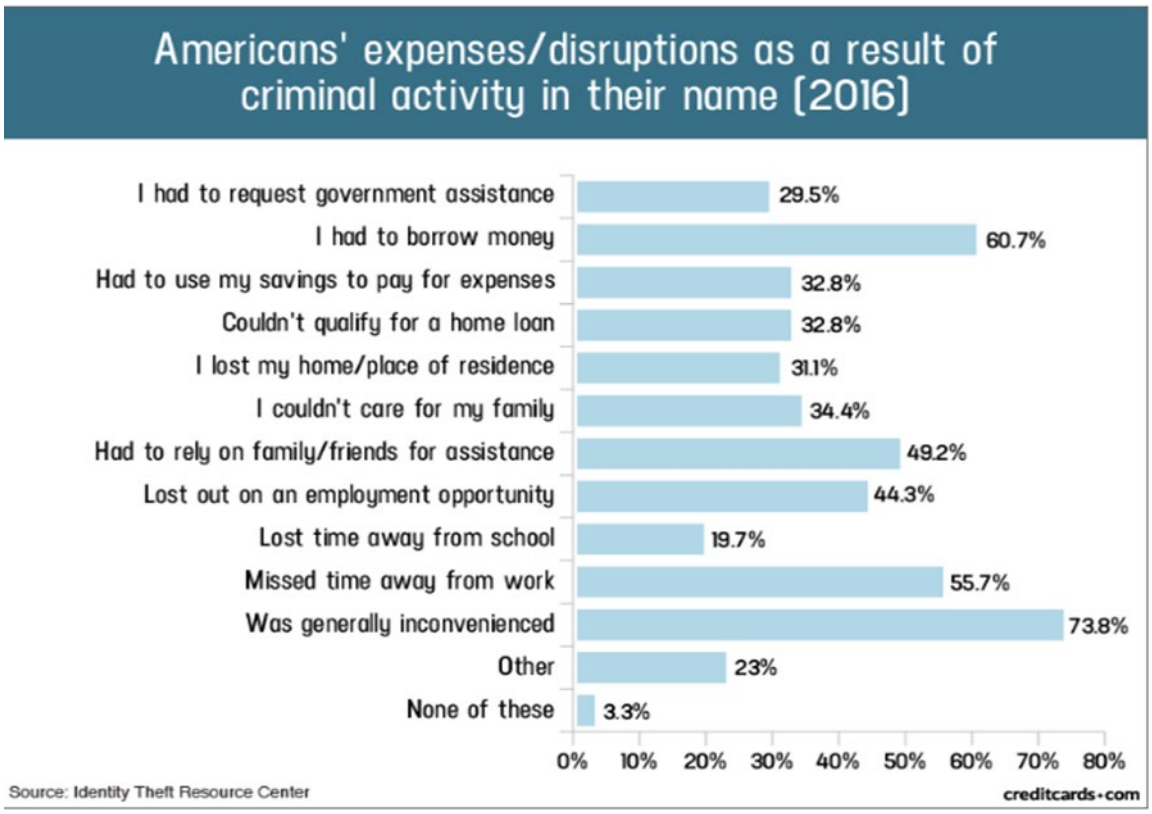
89. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud and bank/finance fraud.

90. 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

[23] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited July 6, 2021).

issued in the victim's name.

91. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[24]



92. Moreover, theft of Private Information is also gravely serious. Perhaps needless to say, but PII and PHI is an extremely valuable property right.[25]

93. 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

---

[24] *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.

[25] *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).

risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

94. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[26]

95. 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.

96. 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.

97. 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 29.

[26] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited July 6, 2021).

98. 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-market" for years.

99. 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 Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

101. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[27] 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.

102. 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.[28] 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.[29]

103. Each of these fraudulent activities is difficult to detect. An individual may not know

---

[27] *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/.

[28] *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 July 6, 2021).

[29] *Id.* at 4.

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 individual's authentic tax return is rejected.

104. Moreover, it is not an easy task to change or cancel a stolen Social Security number. 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."[30]

105. 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."[31]

106. Medical information is especially valuable to identity thieves.

107. 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.[32] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[33]

---

[30] 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.

[31] 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.

[32] *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/.

[33] 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.

108. 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.

109. For this reason, Wolfe knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Wolfe 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.

Plaintiffs' and Class Members' Damages

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

111. The complimentary fraud and identity monitoring service offered by Wolfe is wholly inadequate as the services are only offered for 12 months and it places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

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

113. Plaintiffs' PII and PHI was compromised as a direct and proximate result of the Data Breach.

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

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

116. Plaintiffs 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.

117. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, ransomware and other illegal schemes based on their Private Information.

118. Plaintiffs 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.

119. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach.

120. Numerous courts have recognized the propriety of loss of value damages in related cases.

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

122. In short, Plaintiffs and the Class Members did not get what they paid for.

123. Plaintiffs 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.

124. Plaintiffs 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:

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

q. Purchasing credit monitoring and identity theft prevention;

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

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

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

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

125. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant (in some form), 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.

126. Further, as a result of Wolfe's conduct, Plaintiffs 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.

127. As a direct and proximate result of Wolfe's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at an increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

128. Pursuant to Iowa Rule of Civil Procedure 1.262, Plaintiffs seek certification of the following classes of persons defined as follows:

> **National Class:** All persons Wolfe identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.
>
> **Iowa Sub-Class:** All persons residing in the State of Iowa that Wolfe identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

Excluded from the Classes are any judges presiding over this matter and court personnel assigned to this case.

129. **Numerosity**: The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, the Classes reportedly include approximately 500,000 current and former patients of Wolfe. The identities of Class Members are ascertainable through Wolfe's records, Class Members' records, publication notice, self-identification and other means.

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

a. Whether Wolfe unlawfully used, maintained, lost or disclosed Plaintiffs' and Class Members' Private Information;

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

c. Whether Wolfe's data security systems prior to and during the Cyber-Attack and Data Breach complied with applicable data security laws and regulations, *e.g.*, HIPAA;

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

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

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

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

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

i. Whether Wolfe owed a duty to provide Plaintiffs and Class Members notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Wolfe's misconduct;

k. Whether Wolfe's conduct was negligent;

l. Whether Wolfe's conduct violated federal law;

m. Whether Wolfe's conduct violated state law and

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

131. Common sources of evidence may also be used to demonstrate Wolfe's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Wolfe's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

132. **Typicality**. Plaintiffs' claims are typical of the claims of the respective Class he seeks to represent, in that the named Plaintiffs and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiffs have no interests adverse to the interests of the other members of the Class.

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

134. **Predominance**. Wolfe has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data 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.

135. **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 Wolfe. 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.

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

137. Certification is appropriate 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 Wolfe owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing and safeguarding their Private Information;

b. Whether Wolfe's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Wolfe's failure to institute adequate protective security measures amounted to negligence;

d. Whether Wolfe failed to take commercially reasonable steps to safeguard consumer Private Information and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

138. Finally, all members of the proposed Classes are readily ascertainable. Wolfe 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 Wolfe.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Classes)

139. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-138 as if fully set forth herein.

140. Plaintiffs bring this claim individually and on behalf of the Class Members.

141. In order to receive medical treatments and services, Wolfe and/or its Agents required Plaintiffs and Class Members to submit non-public Private Information, such as PII and PHI.

142. Plaintiffs and Class Members entrusted their Private Information to Wolfe and/or its Agents with the understanding that Wolfe would safeguard their information.

143. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Wolfe 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.

144. Defendant'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.

145. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein and to ensure

that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

146. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as common law.

147. Defendant 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.

148. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

149. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

150. In addition, Defendant 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.

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

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

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

b. Failing to adequately monitor the security of their networks and systems;

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

d. Failing to adequately train its employees to recognize and contain phishing attacks;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

g. Failing to timely notify Class Members about the Cyber-Attack regarding what type of Private Information had been compromised so that they could take appropriate steps to mitigate the potential for identity theft and other damages and

h. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

153. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

154. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

155. 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.

156. Plaintiffs and Class Members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

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

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Classes)

158. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

159. Through their course of conduct, Defendant, Plaintiffs and Class Members entered into implied contracts for the provision of healthcare and treatment, as well as implied contracts for Defendant to implement data security adequate to safeguard andto protect the privacy of Plaintiffs' and Class Members' Private Information.

160. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendant when he first went for medical care and treatment at one of Defendant's facilities.

161. The valid and enforceable implied contracts to provide medical health care services that Plaintiffs and Class Members entered into with Defendant and/or its Agents include the promise to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.

162. When Plaintiffs and Class Members provided their Private Information to Defendant and/or its Agents in exchange for medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

163. Defendant and/or its agents solicited and invited Class Members to provide their

Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

165. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

166. Under the implied contracts, Defendant and/or its Agents promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members and (b) protect Plaintiffs' and the Class Members' PII/PHI: (i) provided to obtain such health care and/or (ii) created as a result of providing such health care. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

167. Both the provision of medical services healthcare and the protection of Plaintiffs' and Class Members' Private Information were material aspects of these implied contracts.

168. The implied contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are also acknowledged, memorialized and embodied in certain documents, including (among other documents) Defendant's Privacy Policy and Notice of Data Incident.

169. Defendant's express representations, including, but not limited to the express representations found in its Privacy Policy, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and to protect the

privacy of Plaintiffs' and Class Members' Private Information.[34]

170. Consumers of healthcare value their privacy, the privacy of their dependents and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

171. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant and/or its Agents and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

172. A meeting of the minds occurred as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and/or its Agents, and paid for the provided healthcare in exchange for, amongst other things, both the provision of health care and medical services and the protection of their Private Information.

173. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

174. Defendant materially breached its contractual obligation to protect the non-public Private Information Defendant gathered when the sensitive information was accessed by unauthorized personnel as part of the Data Breach.

175. Defendant materially breached the terms of the implied contracts, including, but

[34] *See* https://www.wolfeeyeclinic.com/privacy-policy (last visited June 29, 2021).

not limited to, the terms stated in the relevant Privacy Policy.

176. Wolfe did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and approximately 500,000 Class Members.

177. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA or otherwise protect Plaintiffs' and the Class Members' Private Information, as set forth above.

178. The Cyber-Attack and Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

179. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received health care and other medical services that were of a diminished value to that described in the contracts.

180. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the health care they received.

181. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

182. As a direct and proximate result of the Cyber-Attack/Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information,

the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

183. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack/Data Breach.

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

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Classes)

185. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

186. This count is plead in the alternative to the breach of contract count above.

187. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its Agents and in so doing provided Defendant with their Private Information.

188. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

189. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

190. The amount Plaintiffs and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

191. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

192. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

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

194. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to Defendant's services.

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

196. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

198. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Classes)

199. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

200. At all times during Plaintiffs' and Class Members' interactions with Defendant and/or its Agents, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information.

201. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored and protected in confidence, and would not be disclosed to unauthorized third parties.

202. Plaintiffs and Class Members provided their Private Information to Defendant

and/or its Agents with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

203. Plaintiffs and Class Members also provided their Private Information to Defendant and/or its Agents with the explicit and implicit understandings that Defendant would take precautions to protect such Private Information from unauthorized disclosure.

204. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

205. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

206. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

207. But for Defendant's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their protected Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties.

208. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' protected Private Information, as well as the resulting damages.

209. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members'

Private Information.

210. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from medical fraud, financial fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of patients in their continued possession and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

211. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class Members have suffered and will continue to suffer injury and/or harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs ROBERT MYSHKA and DANIEL STUMME, individually and behalf of all others similarly situated, pray for relief as follows:

A. For an Order certifying this case as a class action pursuant to Iowa Rule of Civil Procedure 1.262, appointing Plaintiffs as Class Representatives and the undersigned attorneys as Class Counsel;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to ensure that the Class has an effective remedy, including enjoining Wolfe from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action and

F. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

DATED: July 9, 2021

Respectfully submitted,

/s/ J. Barton Goplerud

J. Barton Goplerud, AT0002983
SHINDLER ANDERSON GOPLERUD & WEESE P.C.
5015 Grand Ridge Drive, Suite 100
West Des Moines, Iowa 50265-5749
Telephone: (515) 223-4567
Facsimile: (515) 223-8887
Email: goplerud@sagwlaw.com

/s/ Brian O. Marty
Brian O. Marty, AT0011622
SHINDLER, ANDERSON, GOPLERUD & WEESE, P.C.
5015 Grand Ridge Drive, Suite 100
West Des Moines, Iowa 50265-5749
Telephone: (515) 223-4567
Facsimile: (515) 223-8887
Email: marty@sagwlaw.com

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

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290
gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiffs & the Proposed Class