

Cristina Perez Hesano (#027023)

cperez@perezlawgroup.com

PEREZ LAW GROUP, PLLC

7508 N. 59th Avenue

Glendale, AZ 85301

Telephone: 602.730.7100

Fax: 623.235.6173

Gary M. Klinger (*pro hac vice forthcoming*)

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN LLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Phone: (866) 252-0878

gklinger@milberg.com

*Attorneys for Plaintiff and
the proposed Class*

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Linda Hulewat, on behalf of herself
individually and on behalf of all others
similarly situated,

Plaintiff,

v.

Medical Management Resource Group,
L.L.C. d/b/a American Vision Partners,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY DEMAND

Plaintiff Linda Hulewat (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Defendant Medical Management Resource Group, L.L.C. d/b/a American Vision Partners (“MMRG” or “Defendant”) as an individual and on behalf of all others similarly

1 situated, and alleges, upon personal knowledge as to her own actions and her counsels'
2 investigation, and upon information and belief as to all other matters, as follows:

3 **NATURE OF THE ACTION**

4 1. This class action arises out of the recent cyberattack and data breach (“Data
5 Breach”) resulting from MMRG's failure to implement reasonable and industry standard data
6 security practices.

7 2. Defendant is an Arizona-based limited liability company that provides
8 administrative services to ophthalmology practices.¹

9 3. Plaintiff brings this Complaint against Defendant for its failure to properly secure
10 and safeguard the sensitive information that it collected and maintained as part of its regular
11 business practices, including, but not limited to names, dates of birth, and contact information
12 (“personally identifying information” or “PII”) and medical treatment and health insurance
13 information, which is protected health information (“PHI”, and collectively with PII, “Private
14 Information”) as defined by the Health Insurance Portability and Accountability Act of 1996
15 (“HIPAA”).

16 4. Upon information and belief, former and current patients at MMRG’s clients are
17 required to entrust Defendant with sensitive, non-public Private Information, without which
18 Defendant could not perform its regular business activities, in order to obtain medical services
19 from Defendant’s clients. Defendant retains this information for at least many years and even
20 after the patient-physician relationship has ended.

21
22
23
24
25
26
27

¹ The “Notice Letter.”

1 5. By obtaining, collecting, using, and deriving a benefit from the Private
2 Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to
3 those individuals to protect and safeguard that information from unauthorized access and
4 intrusion.

5
6 6. According to the untitled letters that Defendant sent to Plaintiff and other
7 impacted Class Members (the "Notice Letter"), on November 14, 2023, Defendant “detected
8 unauthorized activity on certain parts of [its] network.”² In response, Defendant “launched an
9 investigation with the assistance of leading third-party cybersecurity firms[.]”³ As a result of
10 its investigation, Defendant concluded—on or around December 6, 2023—that “the
11 unauthorized party obtained personal information associates with patients of [Defendant’s
12 clients].”⁴

13
14 7. Defendant's investigation concluded that the Private Information compromised in
15 the Data Breach included Plaintiff’s and approximately 2,350,000 other individuals’
16 information.⁵

17
18 8. Defendant failed to adequately protect Plaintiff’s and Class Members’ Private
19 Information—and failed to even encrypt or redact this highly sensitive information. This
20 unencrypted, unredacted Private Information was compromised due to Defendant's negligent
21 and/or careless acts and omissions and their utter failure to protect its clients’ patients’ sensitive
22 data. Hackers targeted and obtained Plaintiff’s and Class Members’ Private Information because
23

24
25 ² *Id.*

26 ³ *Id.*

27 ⁴ *Id.*

⁵ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

1 of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present
2 and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

3 9. In breaching their duties to properly safeguard its clients' patients' Private
4 Information and give patients timely, adequate notice of the Data Breach's occurrence,
5 Defendant's conduct amounts to negligence and/or recklessness and violates federal and state
6 statutes.
7

8 10. Plaintiff brings this action on behalf of all persons whose Private Information was
9 compromised as a result of Defendant's failure to: (i) adequately protect the Private Information
10 of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's
11 inadequate information security practices; and (iii) effectively secure hardware containing
12 protected Private Information using reasonable and effective security procedures free of
13 vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates
14 federal and state statutes.
15
16

17 11. Defendant disregarded the rights of Plaintiff and Class Members by intentionally,
18 willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable
19 measures to ensure that the Private Information of Plaintiff and Class Members was
20 safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and
21 failing to follow applicable, required, and appropriate protocols, policies, and procedures
22 regarding the encryption of data, even for internal use. As a result, the Private Information of
23 Plaintiff and Class Members was compromised through disclosure to an unknown and
24 unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring
25 that their information is and remains safe, and they should be entitled to injunctive and other
26
27

1 equitable relief.

2 12. Plaintiff and Class Members have suffered injuries as a result of Defendant's
3 conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information;
4 (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs
5 associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of
6 benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the
7 actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts,
8 and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and
9 certainly increased risk to their Private Information, which: (a) remains unencrypted and
10 available for unauthorized third parties to access and abuse; and (b) remains backed up in
11 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant
12 fails to undertake appropriate and adequate measures to protect the Private Information.

13
14
15 13. Plaintiff seeks to remedy these harms and prevent any future data compromise on
16 behalf of herself and all similarly situated persons whose personal data was compromised and
17 stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data
18 security practices.
19

20 PARTIES

21
22 14. Plaintiff Linda Hulewat is and has been, at all relevant times, a resident and
23 citizen of Henderson, Nevada.

24 15. Defendant Medical Management Resource Group, L.L.C. d/b/a American Vision
25 Partners is a limited liability company formed under the state laws of Arizona, with its principal
26 place of business located in Maricopa County, Arizona.
27

JURISDICTION AND VENUE

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

17. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Defendant’s principal place of business is located in this district; Defendant maintains Class Members’ Private Information in this District; and Defendant caused harm to Class Members residing in this District.

STATEMENT OF FACTS

Defendant's Business

19. Defendant is an Arizona-based limited liability company that provides administrative services to ophthalmology practices.⁶

20. In order to obtain medical services from Defendant’s clients, Defendant requires its clients’ patients to provide sensitive and confidential Private Information, including their names, insurance information, dates of birth, and other sensitive information.

⁶ Notice Letter.

1 21. The information held by Defendant in its computer systems included the
2 unencrypted Private Information of Plaintiff and Class Members.

3 22. Upon information and belief, Defendant made promises and representations to its
4 clients' patients would be kept safe, confidential, that the privacy of that information would be
5 maintained, and that Defendant would delete any sensitive information after it was no longer
6 required to maintain it.

7 23. Plaintiff and Class Members provided their Private Information to Defendant
8 with the reasonable expectation and mutual understanding that Defendant would comply with
9 its obligations to keep such information confidential and secure from unauthorized access.
10

11 24. Plaintiff and the Class Members have taken reasonable steps to maintain the
12 confidentiality of their Private Information. Plaintiff and Class Members relied on the
13 sophistication of Defendant to keep their Private Information confidential and securely
14 maintained, to use this information for necessary purposes only, and to make only authorized
15 disclosures of this information. Plaintiff and Class Members value the confidentiality of their
16 Private Information and demand security to safeguard their Private Information.
17

18 25. Defendant had a duty to adopt reasonable measures to protect the Private
19 Information of Plaintiff and Class Members from involuntary disclosure to third parties.
20 Defendant has a legal duty to keep patients' Private Information safe and confidential.
21

22 26. Defendant had obligations created by the FTC Act, HIPAA, contract, and
23 industry standards, to keep its clients' patients' Private Information confidential and to protect
24 it from unauthorized access and disclosure.
25

26 27. Defendant derived a substantial economic benefit from collecting Plaintiff's and
27

1 Class Members' Private Information. Without the required submission of Private Information,
2 Defendant could not perform the services it provides.

3 28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class
4 Members' Private Information, Defendant assumed legal and equitable duties and knew or
5 should have known that it was responsible for protecting Plaintiff's and Class Members' Private
6 Information from disclosure.
7

8 ***The Data Breach***

9 29. On or about February 15, 2024, Defendant began sending Plaintiff and other
10 victims of the Data Breach an untitled letter (the "Notice Letter"), informing them, in relevant
11 part, that:
12

13 On November 14, 2023, we detected unauthorized activity on certain parts of our
14 network. Upon learning of the incident, we promptly took steps to contain it, including
15 isolating impacted systems. We also launched an investigation with the assistance of
16 leading third-party cybersecurity firms and coordinated with law enforcement. We
continue to take preventative actions to further safeguard our systems.

17 On or around December 6, 2023, we determined that, in connection with the incident we
18 detected on November 14, the unauthorized party obtained personal information
19 associates with patients of the Practices. The information for affected patients varied and
20 may have included your name, contact information, date of birth, certain medical
information (e.g. services received, clinical records, and medications) and insurance
information.⁷

21 30. Omitted from the Notice Letter were the dates of the Data Breach, the dates of
22 Defendant's investigation, the details of the root cause of the Data Breach, the vulnerabilities
23 exploited, and the remedial measures undertaken to ensure such a breach does not occur again.
24 To date, these critical facts have not been explained or clarified to Plaintiff and Class Members,
25

26
27 ⁷ Notice Letter.

1 who retain a vested interest in ensuring that their Private Information remains protected.

2 31. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with
3 any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts.
4 Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting
5 from the Data Breach is severely diminished.
6

7 32. Defendant did not use reasonable security procedures and practices appropriate
8 to the nature of the sensitive information it was maintaining for Plaintiff and Class Members,
9 causing the exposure of Private Information, such as encrypting the information or deleting it
10 when it is no longer needed.
11

12 33. The attacker accessed and acquired files in Defendant’s computer systems
13 containing unencrypted Private Information of Plaintiff and Class Members, including their
14 names, dates of birth, PHI, and other sensitive information. Plaintiff’s and Class Members’
15 Private Information was accessed and stolen in the Data Breach.
16

17 34. Plaintiff further believes that her Private Information and that of Class Members
18 was or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit
19 cyber-attacks of this type.
20

21 ***Data Breaches Are Preventable***

22 35. As explained by the Federal Bureau of Investigation, “[p]revention is the most
23 effective defense against ransomware and it is critical to take precautions for protection.”⁸
24

25 36. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could
26

27 ⁸ See How to Protect Your Networks from RANSOMWARE, at 3, available at
<https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

1 and should have implemented, as recommended by the United States Government, the
2 following measures:

- 3 ● Implement an awareness and training program. Because end users are targets,
4 employees and individuals should be aware of the threat of ransomware and how
5 it is delivered.
- 6 ● Enable strong spam filters to prevent phishing emails from reaching the end users
7 and authenticate inbound email using technologies like Sender Policy Framework
8 (SPF), Domain Message Authentication Reporting and Conformance (DMARC),
9 and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- 10 ● Scan all incoming and outgoing emails to detect threats and filter executable files
11 from reaching end users.
- 12 ● Configure firewalls to block access to known malicious IP addresses.
- 13 ● Patch operating systems, software, and firmware on devices. Consider using a
14 centralized patch management system.
- 15 ● Set anti-virus and anti-malware programs to conduct regular scans automatically.
- 16 ● Manage the use of privileged accounts based on the principle of least privilege:
17 no users should be assigned administrative access unless absolutely needed; and
18 those with a need for administrator accounts should only use them when
19 necessary.
- 20 ● Configure access controls—including file, directory, and network share
21 permissions—with least privilege in mind. If a user only needs to read specific
22 files, the user should not have write access to those files, directories, or shares.
- 23 ● Disable macro scripts from office files transmitted via email. Consider using
24 Office Viewer software to open Microsoft Office files transmitted via email
25 instead of full office suite applications.
- 26 ● Implement Software Restriction Policies (SRP) or other controls to prevent
27 programs from executing from common ransomware locations, such as
temporary folders supporting popular Internet browsers or
compression/decompression programs, including the AppData/LocalAppData
folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁹

37. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

⁹ *Id.* at 3-4.

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁰

38. Given that Defendant was storing the sensitive Private Information of its clients' current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

39. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of over two million individuals, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, & Stores Plaintiff's and Class Members' Private Information

40. As a condition to obtain medical services from Defendant's clients, Defendant requires its clients' patients to give their sensitive and confidential Private Information to Defendant.

41. Defendant retains and stores this information and derives a substantial economic

¹⁰ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

1 benefit from the Private Information that they collect. But for the collection of Plaintiff's and
2 Class Members' Private Information, Defendant would be unable to perform its services.

3 42. By obtaining, collecting, and storing the Private Information of Plaintiff and Class
4 Members, Defendant assumed legal and equitable duties and knew or should have known that
5 they were responsible for protecting the Private Information from disclosure.
6

7 43. Plaintiff and Class Members have taken reasonable steps to maintain the
8 confidentiality of their Private Information and relied on Defendant to keep their Private
9 Information confidential and maintained securely, to use this information for business purposes
10 only, and to make only authorized disclosures of this information.
11

12 44. Defendant could have prevented this Data Breach by properly securing and
13 encrypting the files and file servers containing the Private Information of Plaintiff and Class
14 Members.
15

16 45. Upon information and belief, Defendant made promises to its clients' patients and
17 other personnel to maintain and protect their Private Information, demonstrating an
18 understanding of the importance of securing Private Information.
19

20 46. Defendant's negligence in safeguarding the Private Information of Plaintiff and
21 Class Members is exacerbated by the repeated warnings and alerts directed to protecting and
22 securing sensitive data.

23 ***Defendant Knew, Or Should Have Known, Of The Risk Because Healthcare Entities***
24 ***In Possession Of Private Information Are Particularly Susceptible To Cyber Attacks***

25 47. Data thieves regularly target companies like Defendant's due to the highly
26 sensitive information that they custody. Defendant knew and understood that unprotected
27

1 Private Information is valuable and highly sought after by criminal parties who seek to illegally
2 monetize that Private Information through unauthorized access.

3 48. Defendant's data security obligations were particularly important given the
4 substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that
5 collect and store Private Information and other sensitive information, like Defendant, preceding
6 the date of the breach.
7

8 49. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced
9 data breaches, resulting in 66,658,764 individuals' personal information being compromised.¹¹
10

11 50. In light of recent high profile cybersecurity incidents at other healthcare partner
12 and provider companies, including American Medical Collection Agency (25 million patients,
13 March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida
14 Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000
15 patients, September 2018), Oregon Department of Human Services (645,000 patients, March
16 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000
17 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew
18 or should have known that its electronic records would be targeted by cybercriminals.
19
20

21 51. Indeed, cyber-attacks, such as the one experienced by Defendant, have become
22 so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have
23 issued a warning to potential targets so they are aware of, and prepared for, a potential attack.
24 As one report explained, smaller entities that store Private Information are "attractive to
25

26
27 ¹¹ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹²

52. Additionally, as companies became more dependent on computer systems to run their business,¹³ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁴

53. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

54. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

55. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class

¹²https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

¹³<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹⁴<https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

1 Members as a result of a breach.

2 56. Defendant was, or should have been, fully aware of the unique type and the
3 significant volume of data on Defendant's server(s), amounting to potentially over two million
4 individuals' detailed, Private Information, and, thus, the significant number of individuals who
5 would be harmed by the exposure of the unencrypted data.
6

7 57. The injuries to Plaintiff and Class Members were directly and proximately caused
8 by Defendant's failure to implement or maintain adequate data security measures for the Private
9 Information of Plaintiff and Class Members.
10

11 58. The ramifications of Defendant's failure to keep secure the Private Information
12 of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—
13 —particularly PHI—fraudulent use of that information and damage to victims may continue for
14 years.
15

16 59. As a healthcare entity in possession of its clients' patients' and other individuals'
17 Private Information, Defendant knew, or should have known, the importance of safeguarding
18 the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable
19 consequences if its data security systems were breached. This includes the significant costs
20 imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed
21 to take adequate cybersecurity measures to prevent the Data Breach.
22

23 ***Value of Private Information***

24 60. The Federal Trade Commission ("FTC") defines identity theft as "a fraud
25 committed or attempted using the identifying information of another person without
26
27

1 authority.”¹⁵ The FTC describes “identifying information” as “any name or number that may
 2 be used, alone or in conjunction with any other information, to identify a specific person,”
 3 including, among other things, “[n]ame, Social Security number, date of birth, official State or
 4 government issued driver’s license or identification number, alien registration number,
 5 government passport number, employer or taxpayer identification number.”¹⁶
 6

7 61. The PII of individuals remains of high value to criminals, as evidenced by the
 8 prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen
 9 identity credentials.¹⁷
 10

11 62. For example, Personal Information can be sold at a price ranging from \$40 to
 12 \$200.¹⁸ Criminals can also purchase access to entire company data breaches from \$900 to
 13 \$4,500.¹⁹
 14

15 63. Theft of PHI is also gravely serious: “[a] thief may use your name or health
 16 insurance numbers to see a doctor, get prescription drugs, file claims with your insurance
 17 provider, or get other care. If the thief’s health information is mixed with yours, your treatment,
 18
 19
 20

21 _____
 22 ¹⁵ 17 C.F.R. § 248.201 (2013).

23 ¹⁶ *Id.*

24 ¹⁷ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

25 ¹⁸ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

26 ¹⁹ *In the Dark*, VPNOverview, 2019, available at:
 27 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

insurance and payment records, and credit report may be affected.”²⁰

64. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient’s complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a “cyber black market” exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

65. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.²¹ Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.²² In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.²³

66. According to account monitoring company LogDog, medical data sells for \$50

²⁰ *Medical I.D. Theft, EFraudPrevention*
<https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.>

²¹ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/>

²² <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/>

²³ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/>

1 and up on the Dark Web.²⁴

2 67. “Medical identity theft is a growing and dangerous crime that leaves its victims
3 with little to no recourse for recovery,” reported Pam Dixon, executive director of World
4 Privacy Forum. “Victims often experience financial repercussions and worse yet, they
5 frequently discover erroneous information has been added to their personal medical files due to
6 the thief’s activities.”²⁵

7 68. A study by Experian found that the average cost of medical identity theft is “about
8 \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-
9 pocket costs for healthcare they did not receive to restore coverage.²⁶ Almost half of medical
10 identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-
11 third of medical identity theft victims saw their insurance premiums rise, and 40 percent were
12 never able to resolve their identity theft at all.²⁷

13 69. Based on the foregoing, the information compromised in the Data Breach is
14 significantly more valuable than the loss of, for example, credit card information in a retailer
15 data breach because, there, victims can cancel or close credit and debit card accounts. The
16 information compromised in this Data Breach is impossible to “close” and difficult, if not
17
18
19
20

21 _____
22 ²⁴ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security
23 (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>

24 ²⁵ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News,
25 Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>

26 ²⁶ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3,
27 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>

²⁷ *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*,
EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>

impossible, to change—names, dates of birth, and PHI.

70. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”²⁸

71. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

72. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁹

73. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

²⁸ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

²⁹ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

Defendant Fails To Comply With FTC Guidelines

74. 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.

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient 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.³⁰

76. 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.³¹

77. The FTC further recommends that companies not maintain Private Information 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

³⁰ *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

³¹ *Id.*

1 implemented reasonable security measures.

2 78. The FTC has brought enforcement actions against businesses for failing to
3 adequately and reasonably protect patient data, treating the failure to employ reasonable and
4 appropriate measures to protect against unauthorized access to confidential patient data as an
5 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),
6 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must
7 take to meet their data security obligations.
8

9 79. These FTC enforcement actions include actions against healthcare entities, like
10 Defendant. *See, e.g., In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (MMRGH) ¶
11 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that
12 LabMD’s data security practices were unreasonable and constitute an unfair act or practice in
13 violation of Section 5 of the FTC Act.”).
14

15 80. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or
16 affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or
17 practice by businesses, such as Defendant, of failing to use reasonable measures to protect
18 Private Information. The FTC publications and orders described above also form part of the
19 basis of Defendant’s duty in this regard.
20

21 81. Defendant failed to properly implement basic data security practices.
22

23 82. Defendant’s failure to employ reasonable and appropriate measures to protect
24 against unauthorized access to its clients’ patients’ Private Information or to comply with
25 applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the
26 FTC Act, 15 U.S.C. § 45.
27

1 83. Upon information and belief, Defendant was at all times fully aware of its
2 obligation to protect the Private Information of its clients' patients, Defendant was also aware
3 of the significant repercussions that would result from its failure to do so. Accordingly,
4 Defendant's conduct was particularly unreasonable given the nature and amount of Private
5 Information it obtained and stored and the foreseeable consequences of the immense damages
6 that would result to Plaintiff and the Class.
7

8 ***Defendant Fails To Comply With HIPAA Guidelines***

9 84. Defendant is a business associate under HIPAA (45 C.F.R. § 160.102) and is
10 required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and
11 Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health
12 Information"), and Security Rule ("Security Standards for the Protection of Electronic
13 Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.
14

15 85. Defendant is subject to the rules and regulations for safeguarding electronic forms
16 of medical information pursuant to the Health Information Technology Act ("HITECH").³² See
17 42 U.S.C. §17921, 45 C.F.R. § 160.103.
18

19 86. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable*
20 *Health Information* establishes national standards for the protection of health information.
21

22 87. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic*
23 *Protected Health Information* establishes a national set of security standards for protecting
24 health information that is kept or transferred in electronic form.
25

26 _____
27 ³² HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining
protected health information. HITECH references and incorporates HIPAA.

1 88. HIPAA requires “compl[iance] with the applicable standards, implementation
2 specifications, and requirements” of HIPAA “with respect to electronic protected health
3 information.” 45 C.F.R. § 164.302.

4 89. “Electronic protected health information” is “individually identifiable health
5 information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45
6 C.F.R. § 160.103.

7 90. HIPAA’s Security Rule requires Defendant to do the following:

- 8
- 9 a. Ensure the confidentiality, integrity, and availability of all
- 10 electronic protected health information the covered entity or business
- 11 associate creates, receives, maintains, or transmits;
- 12
- 13 b. Protect against any reasonably anticipated threats or hazards to the security
- 14 or integrity of such information;
- 15
- 16 c. Protect against any reasonably anticipated uses or disclosures of such
- 17 information that are not permitted; and
- 18 d. Ensure compliance by its workforce.

19 91. HIPAA also requires Defendant to “review and modify the security measures
20 implemented ... as needed to continue provision of reasonable and appropriate protection of
21 electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant is
22 required under HIPAA to “[i]mplement technical policies and procedures for electronic
23 information systems that maintain electronic protected health information to allow access only
24 to those persons or software programs that have been granted access rights.” 45 C.F.R. §
25 164.312(a)(1).
26
27

1 92. HIPAA and HITECH also obligated Defendant to implement policies and
 2 procedures to prevent, detect, contain, and correct security violations, and to protect against
 3 uses or disclosures of electronic protected health information that are reasonably anticipated
 4 but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see*
 5 *also* 42 U.S.C. §17902.

7 93. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires
 8 Defendant to provide notice of the Data Breach to each affected individual “without
 9 unreasonable delay and *in no case later than 60 days following discovery of the breach.*”³³

11 94. HIPAA requires a business associate to have and apply appropriate sanctions
 12 against members of its workforce who fail to comply with the privacy policies and procedures
 13 of the business associate or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45
 14 C.F.R. § 164.530(e).

16 95. HIPAA requires a business associate to mitigate, to the extent practicable, any
 17 harmful effect that is known to the business associate of a use or disclosure of protected health
 18 information in violation of its policies and procedures or the requirements of 45 C.F.R. Part
 19 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

21 96. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department
 22 of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions
 23 in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has
 24 developed guidance and tools to assist HIPAA covered entities in identifying and implementing
 25

26
 27 ³³ Breach Notification Rule, U.S. Dep’t of Health & Human Services,
<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

1 the most cost effective and appropriate administrative, physical, and technical safeguards to
 2 protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis
 3 requirements of the Security Rule.” US Department of Health & Human Services, Security Rule
 4 Guidance Material.³⁴ The list of resources includes a link to guidelines set by the National
 5 Institute of Standards and Technology (NIST), which OCR says “represent the industry
 6 standard for good business practices with respect to standards for securing e-PHI.” US
 7 Department of Health & Human Services, Guidance on Risk Analysis.³⁵

8
 9 ***Defendant Fails To Comply With Industry Standards***

10
 11 97. As noted above, experts studying cyber security routinely identify healthcare
 12 entities in possession of Private Information as being particularly vulnerable to cyberattacks
 13 because of the value of the Private Information which they collect and maintain.

14
 15 98. Several best practices have been identified that, at a minimum, should be
 16 implemented by healthcare entities in possession of Private Information, like Defendant,
 17 including but not limited to: educating all employees; strong passwords; multi-layer security,
 18 including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable
 19 without a key; multi-factor authentication; backup data and limiting which employees can
 20 access sensitive data. Defendant failed to follow these industry best practices, including a
 21 failure to implement multi-factor authentication.

22
 23 99. Other best cybersecurity practices that are standard in the healthcare industry
 24

25
 26 ³⁴ <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

27 ³⁵ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

1 include installing appropriate malware detection software; monitoring and limiting the network
2 ports; protecting web browsers and email management systems; setting up network systems
3 such as firewalls, switches and routers; monitoring and protection of physical security systems;
4 protection against any possible communication system; training staff regarding critical points.
5 Defendant failed to follow these cybersecurity best practices, including failure to train staff.
6

7 100. Defendant failed to meet the minimum standards of any of the following
8 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation
9 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,
10 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
11 for Internet Security's Critical Security Controls (CIS CSC), which are all established standards
12 for Internet Security's Critical Security Controls (CIS CSC), which are all established standards
13 in reasonable cybersecurity readiness.
14

15 101. These foregoing frameworks are existing and applicable industry standards in the
16 healthcare industry, and upon information and belief, Defendant failed to comply with at least
17 one—or all—of these accepted standards, thereby opening the door to the threat actor and
18 causing the Data Breach.
19

20 **COMMON INJURIES & DAMAGES**

21 102. As a result of Defendant's ineffective and inadequate data security practices, the
22 Data Breach, and the foreseeable consequences of Private Information ending up in the
23 possession of criminals, the risk of identity theft to the Plaintiff and Class Members has
24 materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries
25 and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost
26 or diminished value of Private Information; (iv) lost time and opportunity costs associated with
27

1 attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the
2 bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual
3 consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the
4 continued and certainly increased risk to their Private Information, which: (a) remains
5 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
6 backed up in Defendant's possession and is subject to further unauthorized disclosures so long
7 as Defendant fails to undertake appropriate and adequate measures to protect the Private
8 Information.
9

10
11 ***The Data Breach Increases Victims' Risk Of Identity Theft***

12 103. The unencrypted Private Information of Plaintiff and Class Members will end up
13 for sale on the dark web as that is the *modus operandi* of hackers.

14 104. Unencrypted Private Information may also fall into the hands of companies that
15 will use the detailed Private Information for targeted marketing without the approval of Plaintiff
16 and Class Members. Simply, unauthorized individuals can easily access the Private Information
17 of Plaintiff and Class Members.
18

19 105. The link between a data breach and the risk of identity theft is simple and well
20 established. Criminals acquire and steal Private Information to monetize the information.
21 Criminals monetize the data by selling the stolen information on the black market to other
22 criminals who then utilize the information to commit a variety of identity theft related crimes
23 discussed below.
24

25 106. Plaintiff's and Class Members' Private Information is of great value to hackers
26 and cyber criminals, and the data stolen in the Data Breach has been used and will continue to
27

1 be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to
2 profit off their misfortune.

3 107. One such example of criminals piecing together bits and pieces of compromised
4 PII for profit is the development of “Fullz” packages.³⁶

5 108. With “Fullz” packages, cyber-criminals can cross-reference two sources of
6 Private Information to marry unregulated data available elsewhere to criminally stolen data with
7 an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers
8 on individuals.
9

10 109. The development of “Fullz” packages means here that the stolen Private
11 Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and
12 Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers.
13 In other words, even if certain information such as emails, phone numbers, or credit card
14 numbers may not be included in the Private Information that was exfiltrated in the Data Breach,
15
16
17

18 ³⁶ “Fullz” is fraudster speak for data that includes the information of the victim, including, but
19 not limited to, the name, address, credit card information, social security number, date of birth,
20 and more. As a rule of thumb, the more information you have on a victim, the more money that
21 can be made off of those credentials. Fullz are usually pricier than standard credit card
22 credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed
23 out (turning credentials into money) in various ways, including performing bank transactions
24 over the phone with the required authentication details in-hand. Even “dead Fullz,” which are
25 Fullz credentials associated with credit cards that are no longer valid, can still be used for
26 numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim,
27 or opening a “mule account” (an account that will accept a fraudulent money transfer from a
compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical
Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security
(Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-)

1 criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous
2 operators and criminals (such as illegal and scam telemarketers) over and over.

3 110. The existence and prevalence of “Fullz” packages means that the Private
4 Information stolen from the data breach can easily be linked to the unregulated data (like phone
5 numbers and emails) of Plaintiff and the other Class Members.
6

7 111. Thus, even if certain information (such as insurance information) was not stolen
8 in the data breach, criminals can still easily create a comprehensive “Fullz” package.
9

10 112. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to
11 crooked operators and other criminals (like illegal and scam telemarketers).

12 ***Loss Of Time To Mitigate The Risk Of Identity Theft And Fraud***

13 113. As a result of the recognized risk of identity theft, when a Data Breach occurs,
14 and an individual is notified by a company that their Private Information was compromised, as
15 in this Data Breach, the reasonable person is expected to take steps and spend time to address
16 the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a
17 victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit
18 reports could expose the individual to greater financial harm – yet, the resource and asset of
19 time has been lost.
20

21 114. Thus, due to the actual and imminent risk of identity theft, Defendant instructs,
22 in its Notice Letter, Plaintiffs and Class Members to take the following measures to protect
23 themselves: “[w]e encourage you to remain vigilant against incidents of identity theft and fraud
24
25
26
27

1 by monitoring your free credit reports and reviewing your account statements.”³⁷

2 115. Plaintiff and Class Members have spent, and will spend additional time in the
3 future, on a variety of prudent actions, such as researching and verifying the legitimacy of the
4 Data Breach, replacing credit cards, and monitoring their financial accounts for any indication
5 of fraudulent activity, which may take years to detect.
6

7 116. Plaintiff’s mitigation efforts are consistent with the U.S. Government
8 Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”)
9 in which it noted that victims of identity theft will face “substantial costs and time to repair the
10 damage to their good name and credit record.”³⁸
11

12 117. Plaintiff’s mitigation efforts are also consistent with the steps that FTC
13 recommends that data breach victims take several steps to protect their personal and financial
14 information after a data breach, including: contacting one of the credit bureaus to place a fraud
15 alert (consider an extended fraud alert that lasts for seven years if someone steals their identity),
16 reviewing their credit reports, contacting companies to remove fraudulent charges from their
17 accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁹
18

19 118. And for those Class Members who experience actual identity theft and fraud, the
20 United States Government Accountability Office released a report in 2007 regarding data
21 breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial
22
23

24 _____
25 ³⁷ Notice Letter.

26 ³⁸ See United States Government Accountability Office, GAO-07-737, Personal Information:
27 Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However,
the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

³⁹ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

costs and time to repair the damage to their good name and credit record.”^[4]

Diminution Of Value Of PII and PHI

119. PII and PHI are valuable property rights.⁴⁰ Their value is axiomatic, considering the value of Big Data in corporate America and 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.

120. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.⁴¹

121. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁴²

122. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{43,44} Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁴⁵

⁴⁰ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

⁴¹ 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) (“Private Information, 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).

⁴² 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/>

⁴³ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁴⁴ <https://datacoup.com/>

⁴⁵ <https://digi.me/what-is-digime/>

1 123. According to account monitoring company LogDog, medical data sells for \$50
2 and up on the Dark Web.⁴⁶

3 124. As a result of the Data Breach, Plaintiff's and Class Members' Private
4 Information, which has an inherent market value in both legitimate and dark markets, has been
5 damaged and diminished by its compromise and unauthorized release. However, this transfer
6 of value occurred without any consideration paid to Plaintiff or Class Members for their
7 property, resulting in an economic loss. Moreover, the Private Information is now readily
8 available, and the rarity of the Data has been lost, thereby causing additional loss of value.
9

10 125. At all relevant times, Defendant knew, or reasonably should have known, of the
11 importance of safeguarding the Private Information of Plaintiff and Class Members, and of the
12 foreseeable consequences that would occur if Defendant's data security system was breached,
13 including, specifically, the significant costs that would be imposed on Plaintiff and Class
14 Members as a result of a breach.
15

16 126. The fraudulent activity resulting from the Data Breach may not come to light for
17 years.
18

19 127. Plaintiff and Class Members now face years of constant surveillance of their
20 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
21 continue to incur such damages in addition to any fraudulent use of their Private Information .
22

23 128. Defendant was, or should have been, fully aware of the unique type and the
24

25
26 ⁴⁶ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security
27 (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>

1 significant volume of data on Defendants network, amounting to potentially over two million
2 individuals' detailed personal information and, thus, the significant number of individuals who
3 would be harmed by the exposure of the unencrypted data.

4 129. The injuries to Plaintiff and Class Members were directly and proximately caused
5 by Defendant's failure to implement or maintain adequate data security measures for the Private
6 Information of Plaintiff and Class Members.

7
8 ***Future Cost Of Credit And Identity Theft Monitoring Is Reasonable And Necessary***

9 130. Given the type of targeted attack in this case, sophisticated criminal activity, and
10 the type of Private Information involved, there is a strong probability that entire batches of
11 stolen information have been placed, or will be placed, on the black market/dark web for sale
12 and purchase by criminals intending to utilize the Private Information for identity theft crimes
13 –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file
14 false tax returns; take out loans or lines of credit; or file false unemployment claims.
15

16 131. Such fraud may go undetected until debt collection calls commence months, or
17 even years, later. An individual may not know that his or her Private Information was used to
18 file for unemployment benefits until law enforcement notifies the individual's employer of the
19 suspected fraud. Fraudulent tax returns are typically discovered only when an individual's
20 authentic tax return is rejected.
21

22 132. Consequently, Plaintiff and Class Members are at an increased risk of fraud and
23 identity theft for many years into the future.
24

25 133. The retail cost of credit monitoring and identity theft monitoring can cost around
26 \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect
27

1 Class Members from the risk of identity theft that arose from Defendant's Data Breach.

2 ***Loss of Benefit of the Bargain***

3 134. Furthermore, Defendant's poor data security deprived Plaintiff and Class
4 Members of the benefit of their bargain. When agreeing to obtain medical services at
5 Defendant's clients under certain terms, Plaintiff and other reasonable patients understood and
6 expected that Defendant would properly safeguard and protect their Private Information, when
7 in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class
8 Members received medical services of a lesser value than what they reasonably expected to
9 receive under the bargains they struck with Defendant's clients.
10
11

12 **PLAINTIFF'S EXPERIENCE**

13 135. Plaintiff is a former patient at Southwest Eye Center, which, upon information
14 and belief, contracted with Defendant for services. Plaintiff received services at Southwest Eye
15 Center in approximately 2015.
16

17 136. As a condition of obtaining services at Southwest Eye Center, Plaintiff was
18 required to provide Defendant with her Private Information, including her name, health
19 insurance information, date of birth, and other sensitive information.
20

21 137. Upon information and belief, at the time of the Data Breach, Defendant retained
22 Plaintiff's Private Information in its system.

23 138. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff
24 stores any documents containing her Private Information in a safe and secure location. She has
25 never knowingly transmitted unencrypted sensitive Private Information over the internet or any
26 other unsecured source. Had Plaintiff known that Defendant would fail to implement reasonable
27

1 and adequate data security safeguards, she would not have provided her Private Information to
2 Southwest Eye Center or any entity that provided her information, directly or indirectly to
3 Defendant.

4 139. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendant, dated
5 February 15, 2024, informing her that her Private Information was improperly accessed and
6 obtained by unauthorized third parties during the Data Breach, including her name, contact
7 information, date of birth, certain medical information (e.g. services received, clinical records,
8 and medications) and insurance information.
9

10 140. As a result of the Data Breach and at the direction of the Notice Letter, which
11 instructed her to “remain vigilant against incidents of identity theft and fraud by monitoring
12 your free credit reports and reviewing your account statements[,]”⁴⁷ Plaintiff made reasonable
13 efforts to mitigate the impact of the Data Breach, including but not limited to: researching and
14 verifying the legitimacy of the Data Breach, replacing credit cards, and monitoring her financial
15 accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has
16 spent significant time remedying the breach—valuable time Plaintiff otherwise would have
17 spent on other activities, including but not limited to work and/or recreation. This time has been
18 lost forever and cannot be recaptured.
19

20 141. Plaintiff suffered actual injury from having her Private Information compromised
21 as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of
22 her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and
23

24
25
26
27 ⁴⁷ Notice Letter.

1 opportunity costs associated with attempting to mitigate the actual consequences of the Data
2 Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting
3 to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal
4 damages; and (ix) the continued and certainly increased risk to her Private Information, which:
5 (a) remains unencrypted and available for unauthorized third parties to access and abuse; and
6 (b) remains backed up in Defendant's possession and is subject to further unauthorized
7 disclosures so long as Defendant fails to undertake appropriate and adequate measures to
8 protect the Private Information.
9

10
11 142. Plaintiff further suffered actual injury in the form of experiencing an increase in
12 spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data
13 Breach.

14
15 143. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has
16 been compounded by the fact that Defendant has still not fully informed her of key details about
17 the Data Breach's occurrence.

18
19 144. As a result of the Data Breach, Plaintiff anticipates spending considerable time
20 on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

21
22 145. As a result of the Data Breach, Plaintiff is at a present risk and will continue to
be at increased risk of identity theft and fraud for years to come.

23
24 146. Plaintiff has a continuing interest in ensuring that her Private Information, which,
25 upon information and belief, remains backed up in Defendant's possession, is protected and
26 safeguarded from future breaches.
27

CLASS ACTION ALLEGATIONS

147. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach announced by Defendant in February 2024 (the "Class").

148. 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.

149. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

150. 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, upon information and belief, at least 2,350,000 persons were impacted in the Data Breach.⁴⁸

151. 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;

⁴⁸ https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

- 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 breached implied contracts for adequate data security with Plaintiff and Class Members;
- l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiff and Class Members;

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.

152. 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.

153. 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.

154. Predominance. Defendant has 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.

155. 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

1 adjudications with respect to individual Class Members, which would establish incompatible
2 standards of conduct for Defendant. In contrast, the conduct of this action as a class action
3 presents far fewer management difficulties, conserves judicial resources and the parties'
4 resources, and protects the rights of each Class Member.

5
6 156. Defendant has acted on grounds that apply generally to the Class as a whole, so
7 that class certification, injunctive relief, and corresponding declaratory relief are appropriate on
8 a class-wide basis.

9
10 157. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for
11 certification because such claims present only particular, common issues, the resolution of
12 which would advance the disposition of this matter and the parties' interests therein. Such
13 particular issues include, but are not limited to:

- 14 a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due
15 care in collecting, storing, and safeguarding their Private Information;
16
17 b. Whether Defendant's security measures to protect its data systems were
18 reasonable in light of best practices recommended by data security experts;
19
20 c. Whether Defendant's failure to institute adequate protective security measures
21 amounted to negligence;
22
23 d. Whether Defendant failed to take commercially reasonable steps to safeguard
24 consumer Private Information; and
25
26 e. Whether adherence to FTC data security recommendations, and measures
27 recommended by data security experts would have reasonably prevented the
Data Breach.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27

COUNT I
Negligence

7
8

10

11

12

13

14

16
17
18

20
21
22
23
24
25
26
27

1 of a data breach.

2 164. Defendant had a duty to employ reasonable security measures under Section 5
3 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices
4 in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair
5 practice of failing to use reasonable measures to protect confidential data.
6

7 165. Defendant's duty to use reasonable security measures under HIPAA required
8 Defendant to "reasonably protect" confidential data from "any intentional or unintentional
9 use or disclosure" and to "have in place appropriate administrative, technical, and physical
10 safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).
11 Some or all of the healthcare and/or medical information at issue in this case constitutes
12 "protected health information" within the meaning of HIPAA.
13

14 166. For instance, HIPAA required Defendant to notify victims of the Breach within
15 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiff or Class
16 Members of the Data Breach until February 15, 2024 despite, upon information and belief,
17 Defendant knowing shortly after November 14, 2023 that unauthorized persons had accessed
18 and acquired the private, protected, personal information of Plaintiff and the Class.
19

20 167. Defendant owed a duty of care to Plaintiff and Class Members to provide data
21 security consistent with industry standards and other requirements discussed herein, and to
22 ensure that its systems and networks, and the personnel responsible for them, adequately
23 protected the Private Information.
24

25 168. Defendant's duty of care to use reasonable security measures arose as a result
26 of the special relationship that existed between Defendant and its clients' patients. That
27

1 special relationship arose because Plaintiff and the Class entrusted Defendant with their
2 confidential Private Information, a necessary part of being patients at Defendant's clients.

3 169. Defendant's duty to use reasonable care in protecting confidential data arose
4 not only as a result of the statutes and regulations described above, but also because
5 Defendant is bound by industry standards to protect confidential Private Information.
6

7 170. Defendant was subject to an "independent duty," untethered to any contract
8 between Defendant and Plaintiff or the Class.

9 171. Defendant also had a duty to exercise appropriate clearinghouse practices to
10 remove former patients' Private Information it was no longer required to retain pursuant to
11 regulations.
12

13 172. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff
14 and the Class of the Data Breach.
15

16 173. Defendant had and continues to have a duty to adequately disclose that the
17 Private Information of Plaintiff and the Class within Defendant's possession might have
18 been compromised, how it was compromised, and precisely the types of data that were
19 compromised and when. Such notice was necessary to allow Plaintiff and the Class to take
20 steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private
21 Information by third parties.
22

23 174. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other
24 applicable standards, and thus were negligent, by failing to use reasonable measures to
25 protect Class Members' Private Information. The specific negligent acts and omissions
26 committed by Defendant include, but are not limited to, the following:
27

- 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 email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- f. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations,
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

175. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

176. Plaintiff and the Class are within the class of persons that the FTC Act and

1 HIPAA were intended to protect.

2 177. The harm that occurred as a result of the Data Breach is the type of harm the
3 FTC Act and HIPAA were intended to guard against.

4 178. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes
5 negligence.
6

7 179. The FTC has pursued enforcement actions against businesses, which, as a
8 result of their failure to employ reasonable data security measures and avoid unfair and
9 deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.
10

11 180. A breach of security, unauthorized access, and resulting injury to Plaintiff and
12 the Class was reasonably foreseeable, particularly in light of Defendant's inadequate
13 security practices.

14 181. It was foreseeable that Defendant's failure to use reasonable measures to
15 protect Class Members' Private Information would result in injury to Class Members.
16 Further, the breach of security was reasonably foreseeable given the known high frequency
17 of cyberattacks and data breaches in the healthcare industry.
18

19 182. Defendant has full knowledge of the sensitivity of the Private Information and
20 the types of harm that Plaintiff and the Class could and would suffer if the Private
21 Information were wrongfully disclosed.
22

23 183. Plaintiff and the Class were the foreseeable and probable victims of any
24 inadequate security practices and procedures. Defendant knew or should have known of the
25 inherent risks in collecting and storing the Private Information of Plaintiff and the Class,
26 the critical importance of providing adequate security of that Private Information, and the
27

1 necessity for encrypting Private Information stored on Defendant's systems.

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

5 185. Plaintiff and the Class had no ability to protect their Private Information that
6 was in, and possibly remains in, Defendant's possession.

7 186. Defendant was in a position to protect against the harm suffered by Plaintiff
8 and the Class as a result of the Data Breach.

9 187. Defendant's duty extended to protecting Plaintiff and the Class from the risk
10 of foreseeable criminal conduct of third parties, which has been recognized in situations
11 where the actor's own conduct or misconduct exposes another to the risk or defeats
12 protections put in place to guard against the risk, or where the parties are in a special
13 relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures
14 have also recognized the existence of a specific duty to reasonably safeguard personal
15 information.

16 188. Defendant has admitted that the Private Information of Plaintiff and the Class
17 was wrongfully lost and disclosed to unauthorized third persons as a result of the Data
18 Breach.

19 189. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff
20 and the Class, the Private Information of Plaintiff and the Class would not have been
21 compromised.

22 190. There is a close causal connection between Defendant's failure to implement
23
24
25
26
27

1 security measures to protect the Private Information of Plaintiff and the Class and the harm,
2 or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of
3 Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure
4 to exercise reasonable care in safeguarding such Private Information by adopting,
5 implementing, and maintaining appropriate security measures.
6

7 191. As a direct and proximate result of Defendant's negligence, Plaintiff and the
8 Class have suffered and will suffer injury, including but not limited to: (i) invasion of
9 privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private
10 Information; (iv) lost time and opportunity costs associated with attempting to mitigate the
11 actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity
12 costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii)
13 experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix)
14 nominal damages; and (x) the continued and certainly increased risk to their Private
15 Information, which: (a) remains unencrypted and available for unauthorized third parties to
16 access and abuse; and (b) remains backed up in Defendant's possession and is subject to further
17 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
18 measures to protect the Private Information.
19
20
21

22 192. As a direct and proximate result of Defendant's negligence, Plaintiff and the
23 Class have suffered and will continue to suffer other forms of injury and/or harm, including,
24 but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-
25 economic losses.
26

27 193. Additionally, as a direct and proximate result of Defendant's negligence,

1 Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their
2 Private Information, which remain in Defendant's possession and is subject to further
3 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
4 measures to protect the Private Information in its continued possession.

5
6 194. Plaintiff and Class Members are entitled to compensatory and consequential
7 damages suffered as a result of the Data Breach.

8 195. Defendant's negligent conduct is ongoing, in that it still holds the Private
9 Information of Plaintiff and Class Members in an unsafe and insecure manner.

10
11 196. Plaintiff and Class Members are also entitled to injunctive relief requiring
12 Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit
13 to future annual audits of those systems and monitoring procedures; and (iii) continue to
14 provide adequate credit monitoring to all Class Members.

15
16 **COUNT II**
17 **Negligence *Per Se***
18 **(On Behalf of Plaintiff and All Class Members)**

19 197. Plaintiff re-alleges and incorporates by reference all of the allegations
20 contained in paragraphs 1 through 158, as if fully set forth herein.

21 198. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or
22 affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or
23 practice by Defendant of failing to use reasonable measures to protect Private Information.
24 Various FTC publications and orders also form the basis of Defendant's duty.

25
26 199. Defendant's duty to use reasonable security measures under HIPAA required
27 Defendant to "reasonably protect" confidential data from "any intentional or unintentional

1 use or disclosure" and to "have in place appropriate administrative, technical, and physical
2 safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).
3 Some or all of the healthcare and/or medical information at issue in this case constitutes
4 "protected health information" within the meaning of HIPAA.
5

6 200. For instance, HIPAA required Defendant to notify victims of the Breach within
7 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiff or Class
8 Members of the Data Breach until February 15, 2024 despite, upon information and belief,
9 Defendant knowing shortly after November 14, 2023 that unauthorized persons had accessed
10 and acquired the private, protected, personal information of Plaintiff and the Class.
11

12 201. Defendant violated Section 5 of the FTC Act, HIPAA, and similar state statutes
13 by failing to use reasonable measures to protect Private Information and not complying with
14 industry standards. Defendant's conduct was particularly unreasonable given the nature and
15 amount of Private Information obtained and stored and the foreseeable consequences of a data
16 breach on Defendant's systems.
17

18 202. Defendant's violation of Section 5 of the FTC Act, HIPAA, and similar state
19 statutes constitutes negligence *per se*.
20

21 203. Class members are consumers within the class of persons Section 5 of the FTC
22 Act, HIPAA, and similar state statutes were intended to protect.
23

24 204. Moreover, the harm that has occurred is the type of harm the FTC Act, HIPAA,
25 and similar state statutes were intended to guard against. Indeed, the FTC has pursued over fifty
26 enforcement actions against businesses which, as a result of their failure to employ reasonable
27 data security measures and avoid unfair and deceptive practices, caused the same harm suffered

1 by Plaintiff and Class Members.

2 205. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
3 Members have suffered or will suffer injury, including but not limited to: (i) invasion of
4 privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private
5 Information; (iv) lost time and opportunity costs associated with attempting to mitigate the
6 actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity
7 costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii)
8 statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk
9 to their Private Information, which: (a) remains unencrypted and available for unauthorized
10 third parties to access and abuse; and (b) remains backed up in Defendant's possession and is
11 subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate
12 and adequate measures to protect the Private Information.

13
14
15 206. Plaintiff and Class Members have been injured and are entitled to damages in an
16 amount to be proven at trial.
17

18 **COUNT III**
19 **Breach of Third-Party Beneficiary Contract**
20 **(On Behalf of Plaintiff and All Class Members)**

21 207. Plaintiff re-alleges and incorporates by reference all of the allegations
22 contained in paragraphs 1 through 158, as if fully set forth herein.

23 208. Defendant entered into written contracts with its clients, including, upon
24 information and belief, Southwest Eye Center, to provide administrative services.

25 209. In exchange, Defendant agreed, in part, to implement adequate security measures
26 to safeguard the Private Information of Plaintiff and the Class and to timely and adequately
27

1 notify them of the Data Breach.

2 210. These contracts were made expressly for the benefit of Plaintiff and the Class, as
3 Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered
4 into between Defendant and its clients. Defendant knew that, if it were to breach these contracts
5 with its clients, the clients' patients—Plaintiff and Class Members—would be harmed.

6
7 211. Defendant breached the contracts it entered into with its clients by, among other
8 things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols
9 and employee training sufficient to protect Plaintiff's Private Information from unauthorized
10 disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members
11 of the Data Breach.

12
13 212. Plaintiff and the Class were harmed by Defendant's breach of its contracts with
14 its clients, as such breach is alleged herein, and are entitled to the losses and damages they have
15 sustained as a direct and proximate result thereof.

16
17 213. Plaintiff and Class Members are also entitled to their costs and attorney's fees
18 incurred in this action.

19
20 **COUNT IV**
21 **Unjust Enrichment**
(On Behalf of Plaintiff and All Class Members)

22 214. Plaintiff re-alleges and incorporates by reference all of the allegations
23 contained in paragraphs 1 through 158, as if fully set forth herein.

24 215. Plaintiff brings this claim in the alternative to her breach of third-party
25 beneficiary contract claim above.
26
27

1 216. Plaintiff and Class Members conferred a monetary benefit on Defendant.
2 Specifically, they provided Defendant with their Private Information. In exchange, Plaintiff
3 and Class Members should have had their Private Information protected with adequate data
4 security.

5
6 217. Defendant knew that Plaintiff and Class Members conferred a benefit on it in
7 the form their Private Information. Defendant appreciated and accepted that benefit.
8 Defendant profited from these transactions and used the Private Information of Plaintiff and
9 Class Members for business purposes.

10
11 218. Upon information and belief, Defendant funds its data security measures
12 entirely from its general revenue, including payments on behalf of or for the benefit of
13 Plaintiff and some Class Members.

14
15 219. As such, a portion of the payments made for the benefit of or on behalf of
16 Plaintiff and Class Members is to be used to provide a reasonable level of data security, and
17 the amount of the portion of each payment made that is allocated to data security is known
18 to Defendant.

19
20 220. Defendant, however, failed to secure Plaintiff's and Class Members' Private
21 Information and, therefore, did not provide adequate data security in return for the benefit
22 Plaintiff and Class Members provided.

23 221. Defendant would not be able to carry out an essential function of its regular
24 business without the Private Information of Plaintiff and Class Members and derived
25 revenue by using it for business purposes. Plaintiff and Class Members expected that
26 Defendant or anyone in Defendant's position would use a portion of that revenue to fund
27

1 adequate data security practices.

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

4 223. If Plaintiff and Class Members knew that Defendant had not reasonably
5 secured their Private Information, they would not have allowed their Private Information to
6 be provided to Defendant.

7 224. Defendant enriched itself by saving the costs it reasonably should have
8 expended on data security measures to secure Plaintiff's and Class Members' Personal
9 Information. Instead of providing a reasonable level of security that would have prevented
10 the hacking incident, Defendant instead calculated to increase its own profit at the expense
11 of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and
12 diverting those funds to its own profit. Plaintiff and Class Members, on the other hand,
13 suffered as a direct and proximate result of Defendant's decision to prioritize its own profits
14 over the requisite security and the safety of their Private Information.

15 225. Under the principles of equity and good conscience, Defendant should not be
16 permitted to retain the money wrongfully obtained Plaintiff and Class Members, because
17 Defendant failed to implement appropriate data management and security measures that are
18 mandated by industry standards.

19 226. Plaintiff and Class Members have no adequate remedy at law.

20 227. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
21 Members have suffered and will suffer injury, including but not limited to: (i) invasion of
22 privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private
23
24
25
26
27

Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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.

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

229. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff 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 V

Violation of the Arizona Consumer Fraud Act ("ACFA")

Ariz. Rev. Stat. §§ 44-1521, *et seq.*

(On Behalf of Plaintiff and All Class Members)

230. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 158, as if fully set forth herein.

231. The ACFA provides in pertinent part: "The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise,

1 misrepresentation, or concealment, suppression or omission of any material fact with intent that
2 others rely on such concealment, suppression or omission, in connection with the sale or
3 advertisement of any merchandise whether or not any person has in fact been misled, deceived
4 or damaged thereby, is declared to be an unlawful practice.” Ariz. Rev. Stat. § 44-1522.

5
6 232. Plaintiff and Class Members are “persons” as defined by Ariz. Rev. Stat. § 44-
7 1521(6).

8 233. Defendant provides “services” as that term is included in the definition of
9 “merchandise” under Ariz. Rev. Stat. § 44-1521(5), and Defendant is engaged in the “sale” of
10 “merchandise” as defined by Ariz. Rev. Stat. § 44-1521(7).

11
12 234. Defendant engaged in deceptive and unfair acts and practices, misrepresentation,
13 and the concealment, suppression and omission of material facts in connection with the sale
14 and advertisement of “merchandise” (as defined in the ACFA) in violation of the ACFA,
15 including but not limited to the following:
16

- 17 a. Failing to maintain sufficient security to keep Plaintiff’s and Class Members’
18 confidential medical and personal data from being hacked and stolen;
- 19 b. Failing to disclose the Data Breach to Class Members in a timely and accurate
20 manner, in violation of Ariz. Rev. Stat. § 18-552(B);
- 21 c. Misrepresenting material facts, pertaining to the sale of healthcare services by
22 representing that they would maintain adequate data privacy and security
23 practices and procedures to safeguard Class Members’ PHI and PII from
24 unauthorized disclosure, release, data breaches, and theft;
25
26
27

- 1 d. Misrepresenting material facts, in connection with the sale of healthcare services
2 by representing that they did and would comply with the requirements of relevant
3 federal and state laws pertaining to the privacy and security of Class Members’
4 PHI and PII;
5
6 e. Omitting, suppressing, and concealing the material fact of the inadequacy of the
7 data privacy and security protections for Class Members’ PHI and PII;
8
9 f. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the
10 sale of healthcare services by failing to maintain the privacy and security of Class
11 Members’ PHI and PII, in violation of duties imposed by and public policies
12 reflected in applicable federal and state laws, resulting in the Data Breach. These
13 unfair, unlawful, and deceptive acts and practices violated duties imposed by
14 laws, including HIPAA and Section 5 of the FTC Act;
15
16 g. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the
17 sale of healthcare services by failing to disclose the Data Breach to Class
18 Members in a timely and accurate manner; and
19
20 h. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the
21 sale of healthcare services by failing to take proper action following the Data
22 Breach to enact adequate privacy and security measures and protect Class
23 Members’ PHI and PII from further unauthorized disclosure, release, data
24 breaches, and theft.

25
26 235. The above unlawful, unfair, and deceptive acts and practices by Magellan were
27 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to

1 Plaintiff and Class Members that they could not reasonably avoid; this substantial injury
2 outweighed any benefits to consumers or to competition.

3 236. Defendant knew or should have known that their computer systems and data
4 security practices were inadequate to safeguard Class Members' PHI and PII and that risk of a
5 data breach or theft was high, especially in light of the frequency of Data Breaches in the
6 healthcare industry.

7
8 237. Defendant's actions in engaging in the above-named deceptive acts and practices
9 were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of
10 Members of the Class.

11
12 238. As a direct and proximate result of Defendant's deceptive acts and practices,
13 Plaintiff and Class Members suffered an ascertainable loss of money or property, real or
14 personal, as described above, including the loss of their legally protected interest in the
15 confidentiality and privacy of their PHI and PII.

16
17 239. Plaintiff and Class Members seek relief under the ACFA including, but not
18 limited to, injunctive relief, actual damages, treble damages for each willful or knowing
19 violation, and attorneys' fees and costs.

20
21 **PRAYER FOR RELIEF**

22 WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment
23 against Defendant and that the Court grants the following:

- 24 a) For an Order certifying this action as a class action and appointing Plaintiff and
25 her counsel to represent the Class;
26
27 b) For equitable relief enjoining Defendant from engaging in the wrongful

1 conduct complained of herein pertaining to the misuse and/or disclosure of
2 Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete
3 and accurate disclosures to Plaintiff and Class Members;

4 c) For equitable relief compelling Defendant to utilize appropriate methods and
5 policies with respect to consumer data collection, storage, and safety, and to
6 disclose with specificity the type of PII compromised during the Data Breach;

7 d) For injunctive relief requested by Plaintiff, including but not limited to,
8 injunctive and other equitable relief as is necessary to protect the interests of
9 Plaintiff and Class Members, including but not limited to an order:

10 i. Prohibiting Defendant from engaging in the wrongful and unlawful acts
11 described herein;

12 ii. Requiring Defendant to protect, including through encryption, all data
13 collected through the course of its business in accordance with all
14 applicable regulations, industry standards, and federal, state, or local
15 laws;

16 iii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff
17 and Class Members unless Defendant can provide to the Court
18 reasonable justification for the retention and use of such information
19 when weighed against the privacy interests of Plaintiff and Class
20 Members;

21 iv. Requiring Defendant to implement and maintain a comprehensive
22 Information Security Program designed to protect the confidentiality
23
24
25
26
27

- 1 and integrity of the PII of Plaintiff and Class Members;
- 2 v. Prohibiting Defendant from maintaining the PII of Plaintiff and Class
- 3 Members on a cloud-based database;
- 4 vi. Requiring Defendant to engage independent third-party security
- 5 auditors/penetration testers as well as internal security personnel to
- 6 conduct testing, including simulated attacks, penetration tests, and audits
- 7 on Defendant's systems on a periodic basis, and ordering Defendant to
- 8 promptly correct any problems or issues detected by such third-party
- 9 security auditors;
- 10
- 11
- 12 vii. Requiring Defendant to engage independent third-party security
- 13 auditors and internal personnel to run automated security monitoring;
- 14
- 15 viii. Requiring Defendant to audit, test, and train its security personnel
- 16 regarding any new or modified procedures;
- 17
- 18 ix. Requiring Defendant to segment data by, among other things, creating
- 19 firewalls and access controls so that if one area of Defendant's network
- 20 is compromised, hackers cannot gain access to other portions of
- 21 Defendant's systems;
- 22
- 23 x. Requiring Defendant to conduct regular database scanning and securing
- 24 checks;
- 25
- 26 xi. Requiring Defendant to establish an information security training
- 27 program that includes at least annual information security training for
- all customers, with additional training to be provided as appropriate

1 based upon the customers' respective responsibilities with handling
2 personal identifying information, as well as protecting the personal
3 identifying information of Plaintiff and Class Members;

4 xii. Requiring Defendant to routinely and continually conduct internal
5 training and education, and on an annual basis to inform internal security
6 personnel how to identify and contain a breach when it occurs and what
7 to do in response to a breach;

8
9 xiii. Requiring Defendant to implement a system of tests to assess its
10 respective customers' knowledge of the education programs discussed
11 in the preceding subparagraphs, as well as randomly and periodically
12 testing customers' compliance with Defendant's policies, programs, and
13 systems for protecting personal identifying information;

14
15 xiv. Requiring Defendant to implement, maintain, regularly review, and
16 revise as necessary a threat management program designed to
17 appropriately monitor Defendant's information networks for threats,
18 both internal and external, and assess whether monitoring tools are
19 appropriately configured, tested, and updated;

20
21 xv. Requiring Defendant to meaningfully educate all Class Members about
22 the threats that they face as a result of the loss of their confidential
23 personal identifying information to third parties, as well as the steps
24 affected individuals must take to protect themselves; and

25
26 xvi. Requiring Defendant to implement logging and monitoring programs
27

- sufficient to track traffic to and from Defendant's servers; and
- xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.
- e) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- f) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;
- g) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- h) For an award of punitive damages, as allowable by law;
- i) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- j) Pre- and post-judgment interest on any amounts awarded; and
- k) Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all triable issues.

1 Dated: February 23, 2024.

Respectfully submitted,

2 /s/ Christina Perez Hesano

3 Christina Perez Hesano, Esq.

4 **Perez Law Group, PLLC**

5 7508 North 59th Avenue

6 Glendale, Arizona 85301

cperez@perezlawgroup.com

7 Gary M. Klinger*

8 **MILBERG COLEMAN BRYSON**

9 **PHILLIPS GROSSMAN LLC**

10 227 W. Monroe Street, Suite 2100

Chicago, IL 60606

11 Phone: (866) 252-0878

12 *Attorneys for Plaintiff and Proposed Class*

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): Linda Hulewat , ;

County of Residence: Outside the State of Arizona

County Where Claim For Relief Arose: Maricopa

Plaintiff's Atty(s):

Cristina Perez Hesano , Attorney

Perez Law Group, PLLC
7508 N. 59th Avenue
Glendale, Arizona 85301
602-730-7100

Gary M. Klinger , Attorney

Milberg Coleman Bryson Phillips Grossman, LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
866-252-0878

Defendant(s): Medical Management Resource Group, LLC , ;

County of Residence: Maricopa

Defendant's Atty(s):

,

,

IFP REQUESTED

REMOVAL FROM COUNTY, CASE #

II. Basis of Jurisdiction:

4. Diversity (complete item III)

III. Citizenship of Principal Parties(Diversity Cases Only)

Plaintiff:-

2 Citizen of Another State

Defendant:-

1 Citizen of This State

IV. Origin :

1. Original Proceeding

V. Nature of Suit:

190 Other Contract

VI.Cause of Action:

28 U.S.C. 1322(d)

VII. Requested in Complaint

Class Action:

Yes

Dollar Demand:

Jury Demand:

Yes

VIII. This case is not related to another case.

Signature: Cristina Perez Hesano

Date: 2/23/2024

Case 2:24-cv-00377-DJH Document 1-1 Filed 02/23/24 Page 2 of 2

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014