

1 Robert S. Green (State Bar No. 136183)
Emrah M. Sumer (State Bar No. 329181)
2 **GREEN & NOBLIN, P.C.**
2200 Larkspur Landing Circle, Suite 101
3 Larkspur, CA 94939
Telephone: (415) 477-6700
4 Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

5 James Robert Noblin (State Bar No. 114442)
6 **GREEN & NOBLIN, P.C.**
4500 East Pacific Coast Highway
7 Fourth Floor
Long Beach, CA 90804
8 Telephone: (562) 391-2487
Facsimile: (415) 477-6710
9 Email: gnecf@classcounsel.com

10 William B. Federman*
wbf@federmanlaw.com
11 Oklahoma Bar No. 2853
FEDERMAN & SHERWOOD
12 10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
13 Telephone: (405) 235-1560
Facsimile: (405) 239-2112

14 **Pro Hac Vice* application to be submitted
15
16 *Counsel for Plaintiffs and the Proposed Class*

17 **UNITED STATES DISTRICT COURT**
18 **SOUTHERN DISTRICT OF CALIFORNIA**

19 MICHAEL RUMELY, ABIGAIL
20 BEAN, JESSICA JAY, MATIAS
21 SOTO, and GREGORY BAUM,
individually and on behalf of all
22 others similarly situated and on behalf
23 of the general public,

24 Plaintiffs,

25 v.
26 MEDNAX, INC. and PEDIATRIX
MEDICAL GROUP,

27 Defendants.
28

Case No.: '21CV0152 BAS JLB

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Michael Rumely, as legal guardian of minor children whose initials
2 are H.R. and M.R., Abigail Bean, as legal guardian of a minor child whose initials
3 are C.B., Jessica Jay, as legal guardian of a minor child whose initials are B.J.,
4 Matias Soto, as legal guardian of a minor child whose initials are M.S., and
5 Gregory Baum, as legal guardian of a minor child whose initials are A.B.
6 (collectively, “Plaintiffs”), individually and on behalf of all others similarly
7 situated and on behalf of the general public, for their Class Action Complaint,
8 bring this action against Defendants Mednax, Inc. (“MEDNAX”) and Pediatrix
9 Medical Group, a MEDNAX Company (“Pediatrix”) based on personal
10 knowledge and the investigation of counsel and allege as follows:

11 **I. INTRODUCTION**

12 1. With this action, Plaintiffs seek to hold Defendants responsible for
13 the harms they caused H.R., M.R., C.B., B.J., M.S., A.B., and the nearly 1.3
14 million other similarly situated persons in the massive and preventable data breach
15 that took place between June 17, 2020 and June 22, 2020 by which cyber
16 criminals, through a phishing event, infiltrated Defendants’ inadequately protected
17 Microsoft Office 365-hosted business email accounts where sensitive personal
18 information was being kept unprotected (“Data Breach” or “Breach”).¹

19 2. Defendants also experienced a second data breach on the dates of
20 July 2, 2020 and July 3, 2020.²

21 3. The cyber criminals gained access to certain of Defendants’
22 Microsoft Office 365 business email accounts with the apparent intention of
23

24 _____
25 ¹ The Data Breach appears on the U.S. Department of Health and Human
26 Services’ online public breach tool and shows that approximately 1,290,670
27 individuals were affected by the Data Breach. *See*
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Jan. 12,
2021).

28 ²https://www.oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=mednax&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D= (last accessed Jan. 22, 2021).

1 stealing protected personal information and protected health information of over a
2 million individuals, including newborn babies and young children, whose
3 information was stored on Defendants’ computer systems and business email
4 accounts.

5 4. MEDNAX is a physician-led healthcare organization that partners
6 with hospitals, health systems and healthcare facilities to offer clinical services
7 spanning the continuum of care, as well as revenue cycle management, patient
8 engagement and perioperative improvement consulting solutions.³ The Company
9 is registered with the U.S. Security and Exchange Commission

10 5. Pediatrix, a MEDNAX company, is the nation’s largest provider of
11 maternal-fetal, newborn and pediatric subspecialty services and delivers
12 comprehensive, customized health solutions designed to enhance the patient
13 experience.⁴ Pediatrix provides services to 41 states (including California,
14 Oklahoma, Washington, and Texas) and Puerto Rico, employs over 1,975
15 physicians and over 1,050 advanced practice providers.

16 6. MEDNAX and Pediatrix collaborate with their partners and affiliates
17 “to develop customized solutions that benefit hospitals, patients and payors,” and
18 tout on their website that they are “trusted by patients, hospitals, and referring
19 physicians to *take great care of the patient, every day and in every way.*”⁵

20 7. Plaintiffs and Class members were required, as patients of
21 Defendants and their affiliate partners, to provide Defendants with their “Personal
22 and Medical Information” (defined below), with the assurance that such
23 information will be kept safe from unauthorized access. By taking possession and
24 control of Plaintiffs’ and Class members’ Personal and Medical Information,
25
26

27 ³ <https://www.mednax.com/about/> (last accessed January 8, 2021).

28 ⁴ <https://www.mednax.com/about/mednax-companies/> (last accessed Jan. 15, 2021).

⁵ *Id.*

1 Defendants assumed a duty to securely store and protect the Personal and Medical
2 Information of Plaintiffs and the Class.

3 8. Defendants breached this duty and betrayed the trust of Plaintiffs and
4 Class members by failing to properly safeguard and protect their Personal and
5 Medical Information, thus enabling cyber criminals to access, acquire,
6 appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse,
7 and/or view it.

8 9. The Personal and Medical Information at issue includes (i) patient
9 contact information (such as patient name, guarantor name, address, email
10 address, and date of birth); (ii) Social Security number, driver's license number,
11 state identification number, and/or financial account information; (iii) health
12 insurance information (payor name, payor contract dates, policy information
13 including type and deductible amount and subscriber/Medicare/Medicaid
14 number); (iv) medical and/or treatment information (dates of service, location,
15 services requested or procedures performed, diagnosis, prescription information,
16 physician names, and Medical Record Numbers); and (v) billing and claims
17 information (invoices, submitted claims and appeals, and patient account
18 identifiers used by the patient's provider).⁶

19 10. Defendants' misconduct – failing to timely implement adequate and
20 reasonable measures to protect Plaintiffs' Personal and Medical Information,
21 failing to timely detect the Data Breach, failing to take adequate steps to prevent
22 and stop the Data Breach, failing to disclose the material facts that they did not
23 have adequate security practices in place to safeguard the Personal and Medical
24 Information, failing to honor their promises and representations to protect
25 Plaintiffs' and Class members' Personal and Medical Information, and failing to
26 provide timely and adequate notice of the Data Breach – caused substantial harm
27 and injuries to Plaintiffs and Class members across the United States.

28 _____
⁶ <https://www.databreaches.net/?s=mednax> (last accessed January 8, 2021).

1 11. Due to Defendants’ negligence and failures, cyber criminals obtained
2 and now possess everything they need to commit personal and medical identity
3 theft and wreak havoc on the financial and personal lives of nearly 1.3 million
4 individuals, many of which are babies and young children, for decades to come.

5 12. As a result of the Data Breach, Plaintiffs and Class members have
6 already suffered damages. For example, now that their Personal and Medical
7 Information has been released into the criminal cyber domains, Plaintiffs and
8 Class members are at imminent and impending risk of identity theft. This risk will
9 continue for the rest of their lives, as Plaintiffs and Class members are now forced
10 to deal with the danger of identity thieves possessing and using their Personal and
11 Medical Information. Additionally, Plaintiffs and Class members have already lost
12 time and money responding to and mitigating the impact of the Data Breach,
13 which efforts are continuous and ongoing.

14 13. Plaintiffs bring this action individually and on behalf of the Class and
15 seek actual damages, statutory damages, punitive damages, and restitution, with
16 attorney fees, costs, and expenses, under the California Customer Records Act
17 (“CCRA”), Cal. Civ. Code § 1798.80, *et seq.*, California Confidentiality of
18 Medical Information Act (“CMIA”), Cal. Civ. Code § 56, *et seq.*, California’s
19 Unfair Competition Law (“UCL”), Cal. Bus. Prof. Code § 17200, *et seq.*, and
20 other state personal and medical privacy laws and state consumer protection and
21 unfair and deceptive practices acts, and further sue Defendants for, among other
22 causes of action, negligence (including negligence *per se*). Plaintiffs also seek
23 declaratory and injunctive relief, including significant improvements to
24 Defendants’ data security systems and protocols, future annual audits, Defendant-
25 funded long-term credit monitoring services, and other remedies as the Court sees
26 necessary and proper. incurred in bringing this action, and all other remedies this
27 Court deems proper.

28

1 **II. THE PARTIES**

2 14. Michael Rumely (“Plaintiff Rumely”) is the legal guardian of H.R.
3 and M.R. and they are citizens and residents of California.

4 15. Plaintiff Rumely’s minor children were patients of, and received,
5 medical services from, Defendants.

6 16. Abigail Bean (“Plaintiff Bean”) is the legal guardian of C.B. and they
7 are citizens and residents of Oklahoma.

8 17. Plaintiff Bean’s minor child, C.B., was a patient of, and received
9 medical services from, Defendants.

10 18. Jessica Jay (“Plaintiff Jay”) is the legal guardian of B.J. and they are
11 citizens and residents of Washington.

12 19. Plaintiff Jay’s minor child, B.J., was a patient of, and received
13 medical services from, Defendants.

14 20. Matias Soto (“Plaintiff Soto”) is the legal guardian of M.S. and they
15 are citizens and residents of Texas.

16 21. Plaintiff Soto’s minor child, M.S., was a patient of, and received
17 medical services from, Defendants.

18 22. Gregory Baum (“Plaintiff Baum”) is the legal guardian of A.B. and
19 they are citizens and residents of Oklahoma.

20 23. Plaintiff Baum’s minor child, A.B., was a patient of, and received
21 medical services from, Defendants.

22 24. Plaintiff Baum has reached out to Defendants in an attempt to resolve
23 the dangers A.B. now faces, but Defendants have gone silent.

24 25. Plaintiffs received letters from MEDNAX dated December 16, 2020,
25 informing them that their minor children’s name, address, date of birth, health
26 insurance information (including payor name, payor contract dates, policy
27 information including type and deductible amount and
28 subscriber/Medicare/Medicaid number), medical and/or treatment information

1 (including dates of service, location, services requested or procedures performed,
2 diagnosis, prescription information, physician names and Medical Record
3 Numbers), and billing and claims information were compromised in the Data
4 Breach. *See Exhibit 1*, the “Notice.”

5 26. As required in order to obtain medical services from Defendants,
6 Plaintiffs provided them with highly sensitive personal, health, and insurance
7 information, including their children’s Personal and Medical Information.

8 27. Because of Defendants’ negligence leading up to and including the
9 period of the Data Breach, H.R.’s, M.R.’s, C.B.’s, B.J.’s, M.S.’s and A.B.’s
10 Personal and Medical Information is now in the hands of cyber criminals and
11 H.R., M.R., C.B., B.J., M.S., and A.B. are under an imminent and substantially
12 likely risk of identity theft and fraud, including medical identity theft and medical
13 fraud.

14 28. The imminent risk of medical identity theft and fraud that these
15 children now face is substantial, certainly impending, and continuous and ongoing
16 because of the negligence of Defendants, which negligence led to the Data Breach.
17 Plaintiffs have already been forced to spend time and money, on behalf of their
18 minor children, responding to the Data Breach in an attempt to mitigate the harms
19 of the Breach and determine how best to protect them from identity theft and
20 medical information fraud. These efforts are continuous and ongoing.

21 29. As a direct and proximate result of the Data Breach, Plaintiffs either
22 have purchased or will purchase a yearly subscription to identity theft protection
23 and credit monitoring in order to protect their children from medical identity theft
24 and other types of fraud, of which they are now substantially at risk. This
25 subscription will need to be renewed yearly for the rest of H.R.’s, M.R.’s, C.B.’s,
26 B.J.’s, M.S.’s and A.B.’s lives.

27 30. The children have also suffered injury directly and proximately
28 caused by the Data Breach, including damages and diminution in value of their

1 Personal and Medical Information that was entrusted to Defendants for the sole
2 purpose of obtaining medical services necessary for their health and well-being,
3 with the understanding that Defendants would safeguard this information against
4 disclosure. Additionally, Plaintiffs' Personal and Medical Information is at
5 continued risk of compromise and unauthorized disclosure as it remains in the
6 possession of Defendants and is subject to further breaches so long as Defendants
7 fail to undertake appropriate and adequate measures to protect it.

8 31. H.R., M.R., C.B., B.J., M.S., and A.B. have never been victims of
9 any type of identity theft. To Plaintiffs' knowledge, the Personal and Medical
10 Information compromised in this Data Breach has not been compromised in any
11 prior data breach.

12 32. For the avoidance of doubt, all references made in this Complaint to
13 "Plaintiffs' Personal and Medical Information" are to be interpreted as referring to
14 the Personal and Medical Information of H.R., M.R., C.B., B.J., M.S., and A.B.

15 33. Founded in 1979, Defendants are physician-led healthcare
16 organizations that partner with hospitals, health systems and healthcare facilities
17 to offer clinical services spanning the continuum of care, as well as revenue cycle
18 management, patient engagement and perioperative improvement consulting
19 solutions.

20 34. As part of Defendants' business, Defendants collect substantial
21 amounts of Personal and Medical Information. The information Defendants collect
22 qualifies as "Personal information" under the CCRA and other state data breach
23 and information privacy acts. The medical information that Defendants collect
24 qualifies as "Medical Information" under the federal Health Information
25 Portability and Accountability Act ("HIPAA"), the CMIA, and other state medical
26 record protection acts.

27 35. Defendant MEDNAX and Defendant Pediatrix are both
28 headquartered in Sunrise, Florida.

1 **III. JURISDICTION AND VENUE**

2 36. This Court has diversity jurisdiction over this action under the Class
3 Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action
4 involving more than 100 class members, the amount in controversy exceeds
5 \$5,000,000, exclusive of interest and costs, and Plaintiffs and members of the
6 Class are citizens of states that differ from Defendants.

7 37. This Court has personal jurisdiction over Defendants because
8 Defendants conduct business in and have sufficient minimum contacts with
9 California.

10 38. Venue is likewise proper as to Defendants in this District under 28
11 U.S.C. § 1391(a)(1) because a substantial part of the events or omissions giving
12 rise to the claims asserted herein occurred in this District. Defendants conduct
13 business through this District (including promoting, selling, marketing, and
14 distributing the MEDNAX and Pediatrix brands and services at issue).

15 **IV. FACTUAL ALLEGATIONS**

16 **A. The California Attorney General Notice**

17 39. On or about June 19, 2020, Defendants discovered that unauthorized
18 third-party hackers gained access to certain Microsoft Office 365-hosted business
19 email accounts through a successful phishing event.

20 40. Defendants began filing with various state Attorneys General
21 (including California) sample “Notice of Data Security Incident” letters that
22 mirrored the language of the Notice sent to Plaintiffs and Class members.

23 41. The sample “Notice of Data Security Incident” letter was filed with
24 the Attorney General of California in accordance with California Civ. Code §
25 1798.82(f).

26 42. Pursuant to California Civ. Code § 1798.82(f), “[a] person or
27 business that is required to issue a security breach notification pursuant to
28 [§ 1798.82(a)] to more than 500 California residents as a result of a single breach

1 of the security system shall electronically submit a single sample copy of that
2 security breach notification, excluding any personally identifiable information, to
3 the Attorney General.”

4 43. Plaintiffs’ and Class members’ Personal and Medical Information is
5 “personal information” as defined by California Civ. Code § 1798.82(h).

6 44. Pursuant to California Civ. Code § 1798.82(a)(1), data breach
7 notification letters are sent to residents of California “whose unencrypted
8 personal information was, or is reasonably believed to have been, acquired by an
9 unauthorized person” due to a “breach of the security of the system.”

10 45. California Civ. Code § 1798.82(g) defines “breach of the security of
11 the system” as the “unauthorized acquisition of computerized data that
12 compromises the security, confidentiality, or integrity of personal information
13 maintained by the person or business.”

14 46. The Data Breach was a “breach of the security of the system” as
15 defined by California Civ. Code § 1798.82(g).

16 47. Plaintiffs’ and Class members’ unencrypted personal information was
17 acquired by an unauthorized person or persons as a result of the Data Breach.

18 48. Defendants reasonably believe Plaintiffs’ and Class members’
19 unencrypted personal information was acquired by an unauthorized person as a
20 result of the Data Breach.

21 49. The security, confidentiality, or integrity of Plaintiffs’ and Class
22 members’ unencrypted personal information was compromised as a result of the
23 Data Breach.

24 50. Defendants reasonably believe the security, confidentiality, or
25 integrity of Plaintiffs’ and Class members’ unencrypted personal information was
26 compromised as a result of the Data Breach.

27
28

1 51. Plaintiffs’ and Class members’ unencrypted personal information that
2 was acquired by an unauthorized person as a result of the Data Breach was viewed
3 by unauthorized persons.

4 52. Defendants reasonably believe Plaintiffs’ and Class members’
5 unencrypted personal information that was acquired by an unauthorized person as
6 a result of the Data Breach was viewed by unauthorized persons.

7 53. It is reasonable to infer that Plaintiffs’ and Class members’
8 unencrypted personal information that was acquired by an unauthorized person as
9 a result of the Data Breach was viewed by unauthorized persons.

10 54. It should be presumed that Plaintiffs’ and Class members’
11 unencrypted personal information that was acquired by an unauthorized person as
12 a result of the Data Breach was viewed by unauthorized persons.

13 55. After receiving letters sent pursuant to California Civ. Code §
14 1798.82(a)(1) – and filed with the Attorney General of California in accordance
15 with California Civ. Code § 1798.82(f) – it is reasonable for recipients, including
16 Plaintiffs and Class members in this case, to believe that future harm (including
17 identity theft) is real and imminent, and to take steps to mitigate that risk of future
18 harm.

19 **B. The U.S. Department of Health and Human Services Breach**
20 **Report**

21 56. A breach report regarding the Data Breach filed by Defendants with
22 the Secretary of the U.S. Department of Health and Human Services states that
23 1,290,670 individuals were impacted by the Data Breach (the “Breach Report”).
24 The Breach Report also characterizes the Data Breach as a “hacking/IT incident”
25 and further indicates that the breached information was accessed through email.

26 57. The Breach Report was filed in accordance with 45 CFR §
27 164.408(a).
28

1 58. Plaintiffs’ and Class members’ Personal and Medical Information is
2 “protected health information” as defined by 45 CFR § 160.103.

3 59. Pursuant to 45 CFR § 164.408(a), breach reports are filed with the
4 Secretary of the U.S. Department of Health and Human Services “following the
5 discovery of a breach of unsecured protected health information.”

6 60. 45 CFR § 164.402 defines “breach” as “the acquisition, access, use,
7 or disclosure of protected health information in a manner not permitted under
8 subpart E of this part which compromises the security or privacy of the protected
9 health information.”

10 61. 45 CFR § 164.402 defines “unsecured protected health information”
11 as “protected health information that is not rendered unusable, unreadable, or
12 indecipherable to unauthorized persons through the use of a technology or
13 methodology specified by the [HHS] Secretary[.]”

14 62. Plaintiffs’ and Class members’ Personal and Medical Information is
15 “unsecured protected health information” as defined by 45 CFR § 164.402.

16 63. Plaintiffs’ and Class members’ unsecured protected health
17 information has been acquired, accessed, used, or disclosed in a manner not
18 permitted under 45 CFR Subpart E as a result of the Data Breach.

19 64. Defendants reasonably believe Plaintiffs’ and Class members’
20 unsecured protected health information has been acquired, accessed, used, or
21 disclosed in a manner not permitted under 45 CFR Subpart E as a result of the
22 Data Breach.

23 65. Plaintiffs’ and Class members’ unsecured protected health
24 information acquired, accessed, used, or disclosed in a manner not permitted under
25 45 CFR Subpart E as a result of the Data Breach was not rendered unusable,
26 unreadable, or indecipherable to unauthorized persons.

27 66. Defendants reasonably believe Plaintiffs’ and Class members’
28 unsecured protected health information acquired, accessed, used, or disclosed in a

1 manner not permitted under 45 CFR Subpart E as a result of the Data Breach was
2 not rendered unusable, unreadable, or indecipherable to unauthorized persons.

3 67. Plaintiffs' and Class members' unsecured protected health
4 information that was acquired, accessed, used, or disclosed in a manner not
5 permitted under 45 CFR Subpart E as a result of the Data Breach, and which was
6 not rendered unusable, unreadable, or indecipherable to unauthorized persons, was
7 viewed by unauthorized persons.

8 68. Plaintiffs' and Class members' unsecured protected health
9 information was viewed by unauthorized persons in a manner not permitted under
10 45 CFR Subpart E as a result of the Data Breach.

11 69. Defendants reasonably believe Plaintiffs' and Class members'
12 unsecured protected health information was viewed by unauthorized persons in a
13 manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

14 70. It is reasonable to infer that Plaintiffs' and Class members' unsecured
15 protected health information that was acquired, accessed, used, or disclosed in a
16 manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and
17 which was not rendered unusable, unreadable, or indecipherable to unauthorized
18 persons, was viewed by unauthorized persons.

19 71. It should be presumed that unsecured protected health information
20 acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR
21 Subpart E, and which was not rendered unusable, unreadable, or indecipherable to
22 unauthorized persons, was viewed by unauthorized persons.

23 72. After receiving notice that they were victims of a data breach that
24 required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it
25 is reasonable for recipients of that notice, including Plaintiffs and Class members
26 in this case, to believe that future harm (including identity theft) is real and
27 imminent, and to take steps to mitigate that risk of future harm.

28

1 **C. The Data Breach and Defendants’ Failed Response**

2 73. It is apparent from the Notice sent to Plaintiffs and the Class and
3 from the sample “Notice of Data Security Incident” letters sent to state Attorneys
4 General that the Personal and Medical Information contained within these Office
5 365 accounts was not encrypted.

6 74. Following the phishing event, Defendants began working with a
7 forensic firm to investigate the Breach. Based upon the investigation, the hackers
8 were able to access certain business email accounts between the dates of June 17,
9 2020 and June 22, 2020 where Plaintiffs’ and Class members’ Personal and
10 Medical Information was being held, unencrypted and unprotected.

11 75. Defendants have also reported a subsequent data breach that took
12 place from July 2, 2020 to July 3, 2020.

13 76. Upon information and belief, the unauthorized third-party gained
14 access to the Personal and Medical Information and has engaged in (and will
15 continue to engage in) misuse of the Personal and Medical Information, including
16 marketing and selling Plaintiffs’ and Class members’ Personal and Medical
17 Information on the dark web.

18 77. Despite knowing that over 1 million patients across the nation were in
19 danger as a result of the Data Breach, Defendants did nothing to warn Plaintiffs or
20 Class members until six months after learning of the Data Breach – an
21 unreasonable amount of time under any objective standard.

22 78. Apparently, Defendants chose to complete their investigation and
23 develop a list of talking points before giving Plaintiffs and Class members the
24 information they needed to protect themselves against fraud and identity theft.

25 79. In spite of the severity of the Data Breach, Defendants have done
26 very little to protect Plaintiffs and the Class, which is obvious by the subsequent
27 data breach in July 2020 and the lack of assistance offered to Plaintiffs and the
28 Class. For example, in the Notice, Defendants only encourage victims “to

1 carefully review credit reports and statements sent from providers as well as
2 [victims'] insurance compan[ies] to ensure that all account activity is valid.” The
3 Notice also mentions a free credit reporting service Plaintiffs and Class members,
4 many of which are children, can contact but fails to offer any free identity theft
5 monitoring service to a majority of the Class.⁷

6 80. In effect, Defendants are shirking their responsibility for the harm
7 and increased risk of harm they have caused Plaintiffs and members of the Class,
8 including the distress and financial burdens the Data Breach has placed upon the
9 shoulders of the Data Breach victims.

10 81. Defendants failed to adequately safeguard Plaintiffs' and Class
11 members' Personal and Medical Information, allowing cyber criminals to access
12 this wealth of priceless information for nearly six months before warning the
13 criminals' victims to be on the lookout, and now offer them no remedy or relief.

14 82. Defendants failed to spend sufficient resources on monitoring
15 external incoming emails and training their employees to identify email-borne
16 threats and defend against them.

17 83. Defendants had obligations created by HIPAA, the CMIA, reasonable
18 industry standards, common law, state statutory law, and their assurances and
19 representations to their patients to keep patients' Personal and Medical
20 Information confidential and to protect such Personal and Medical Information
21 from unauthorized access.

22 84. Plaintiffs and Class members were required to provide their Personal
23 and Medical Information to Defendants with the reasonable expectation and
24 mutual understanding that they would comply with their obligations to keep such
25 information confidential and secure from unauthorized access.

26 _____
27 ⁷ For a very limited number of patients or guarantors whose Social Security
28 numbers, driver's license numbers, non-resident and alien registration numbers,
and/or financial account information was compromised, Defendants arranged to
offer complimentary identity monitoring services. *See*
<https://emailevent.kroll.com/> (last accessed Jan. 13, 2021).

1 85. The stolen Personal and Medical Information at issue has great value
2 to the hackers, due to the large number of individuals affected and the fact that
3 health insurance information and Social Security numbers were part of the data
4 that was compromised.

5 **D. Defendants had an Obligation to Protect Personal and Medical**
6 **Information under Federal Law and the Applicable Standard**
7 **of Care**

8 86. Defendants are covered by HIPAA (45 C.F.R. § 160.102). As such,
9 they are required to comply with the HIPAA Privacy Rule and Security Rule, 45
10 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of
11 Individually Identifiable Health Information”), and Security Rule (“Security
12 Standards for the Protection of Electronic Protected Health Information”), 45
13 C.F.R. Part 160 and Part 164, Subparts A and C.

14 87. HIPAA’s Privacy Rule or *Standards for Privacy of Individually*
15 *Identifiable Health Information* establishes national standards for the protection of
16 health information.

17 88. HIPAA’s Privacy Rule or *Security Standards for the Protection of*
18 *Electronic Protected Health Information* establishes a national set of security
19 standards for protecting health information that is kept or transferred in electronic
20 form.

21 89. HIPAA requires Defendants to “comply with the applicable
22 standards, implementation specifications, and requirements” of HIPAA “with
23 respect to electronic protected health information.” 45 C.F.R. § 164.302.

24 90. “Electronic protected health information” is “individually identifiable
25 health information ... that is (i) transmitted by electronic media; maintained in
26 electronic media.” 45 C.F.R. § 160.103.

27 91. HIPAA’s Security Rule requires Defendants to do the following:
28

- 1 a. Ensure the confidentiality, integrity, and availability of all
- 2 electronic protected health information the covered entity or
- 3 business associate creates, receives, maintains, or transmits;
- 4 b. Protect against any reasonably anticipated threats or hazards to
- 5 the security or integrity of such information;
- 6 c. Protect against any reasonably anticipated uses or disclosures of
- 7 such information that are not permitted; and
- 8 d. Ensure compliance by their workforce.

9 92. HIPAA also requires Defendants to “review and modify the security
10 measures implemented ... as needed to continue provision of reasonable and
11 appropriate protection of electronic protected health information.” 45 C.F.R. §
12 164.306(e).

13 93. HIPAA also requires Defendants to “[i]mplement technical policies
14 and procedures for electronic information systems that maintain electronic
15 protected health information to allow access only to those persons or software
16 programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

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

21 95. Defendants were also prohibited by the Federal Trade Commission
22 Act (the “FTC Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts
23 or practices in or affecting commerce.” The Federal Trade Commission (the
24 “FTC”) has concluded that a company’s failure to maintain reasonable and
25 appropriate data security for consumers’ sensitive personal information is an
26

27 _____
28 ⁸ 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 “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham*
2 *Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

3 96. As described before, Defendants are also required (by the CCRA,
4 CMIA and various other states’ laws and regulations) to protect Plaintiffs’ and
5 Class members’ Personal and Medical Information, and further, to handle any
6 breach of the same in accordance with applicable breach notification statutes.

7 97. In addition to their obligations under federal and state laws,
8 Defendants owed a duty to Plaintiffs and Class members to exercise reasonable
9 care in obtaining, retaining, securing, safeguarding, deleting, and protecting the
10 Personal and Medical Information in their possession from being compromised,
11 lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a
12 duty to Plaintiffs and Class members to provide reasonable security, including
13 consistency with industry standards and requirements, and to ensure that their
14 computer systems, networks, and protocols adequately protected the Personal and
15 Medical Information of the Class.

16 98. Defendants owed a duty to Plaintiffs and the Class to design,
17 maintain, and test their computer and email systems to ensure that the Personal
18 and Medical Information in Defendants’ possession was adequately secured and
19 protected.

20 99. Defendants owed a duty to Plaintiffs and the Class to create and
21 implement reasonable data security practices and procedures to protect the
22 Personal and Medical Information in their possession, including adequately
23 training their employees and others who accessed Personal Information within
24 their computer systems on how to adequately protect Personal and Medical
25 Information.

26 100. Defendants owed a duty to Plaintiffs and the Class to implement
27 processes that would detect a breach on their data security systems in a timely
28 manner.

1 101. Defendants owed a duty to Plaintiffs and the Class to act upon data
2 security warnings and alerts in a timely fashion.

3 102. Defendants owed a duty to Plaintiffs and the Class to adequately train
4 and supervise their employees to identify and avoid any phishing emails that make
5 it past their email filtering service.

6 103. Defendants owed a duty to Plaintiffs and the Class to disclose if their
7 computer systems and data security practices were inadequate to safeguard
8 individuals' Personal and Medical Information from theft because such an
9 inadequacy would be a material fact in the decision to entrust Personal and
10 Medical Information with Defendants.

11 104. Defendants owed a duty to Plaintiffs and the Class to disclose in a
12 timely and accurate manner when data breaches occurred.

13 105. Defendants owed a duty of care to Plaintiffs and the Class because
14 they were foreseeable and probable victims of any inadequate data security
15 practices.

16 **E. Defendants were on Notice of Cyber Attack Threats in the**
17 **Healthcare Industry and of the Inadequacy of their Data**
Security

18 106. Defendants were on notice that companies in the healthcare industry
19 were targets for cyberattacks.

20 107. Defendants were on notice that the FBI has recently been concerned
21 about data security in the healthcare industry. In August 2014, after a cyberattack
22 on Community Health Systems, Inc., the FBI warned companies within the
23 healthcare industry that hackers were targeting them. The warning stated that
24 “[t]he FBI has observed malicious actors targeting healthcare related systems,
25 perhaps for the purpose of obtaining the Protected Healthcare Information (PHI)
26 and/or Personally Identifiable Information (PII).”⁹

27 _____
28 ⁹ Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*,
REUTERS (Aug. 2014), <http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820>.

1 108. The American Medical Association (“AMA”) has also warned
2 healthcare companies about the importance of protecting their patients’
3 confidential information:

4 Cybersecurity is not just a technical issue; it’s a patient safety
5 issue. AMA research has revealed that 83% of physicians
6 work in a practice that has experienced some kind of
7 cyberattack. Unfortunately, practices are learning that
8 cyberattacks not only threaten the privacy and security of
9 patients’ health and financial information, but also patient
10 access to care.¹⁰

11 109. As implied by the above quote from the AMA, stolen Personal and
12 Medical Information can be used to interrupt important medical services
13 themselves. This is an imminent and certainly impending risk for Plaintiffs and
14 Class members.

15 110. Defendants were on notice that the federal government has been
16 concerned about healthcare company data encryption. Defendants knew they kept
17 protected health information in their email accounts and yet it appears Defendants
18 did not encrypt these email accounts.

19 111. The United States Department of Health and Human Services’ Office
20 for Civil Rights urges the use of encryption of data containing sensitive personal
21 information. As long ago as 2014, the Department fined two healthcare companies
22 approximately two million dollars for failing to encrypt laptops containing
23 sensitive personal information. In announcing the fines, Susan McAndrew, the
24 DHHS’s Office of Human Rights’ deputy director of health information privacy,
25
26

27 ¹⁰Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics,*
28 *hospitals*, AM. MED. ASS’N (Oct. 4, 2019), <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals>.

1 stated “[o]ur message to these organizations is simple: encryption is your best
2 defense against these incidents.”¹¹

3 112. As covered entities or business associates under HIPAA, Defendants
4 should have known about their weakness toward email-related threats and sought
5 better protection for the Personal and Medical Information accumulating in their
6 employees’ business email accounts.

7 113. In the healthcare industry, the number one threat vector from a cyber
8 security standpoint is phishing. Cybersecurity firm Proofpoint reports that
9 “phishing is the initial point of compromise in most significant [healthcare]
10 security incidents, according to a recent report from the Healthcare Information
11 and Management Systems Society (HIMSS). And yet, 18% of healthcare
12 organizations fail to conduct phishing tests, a finding HIMSS describes as
13 ‘incredible.’”¹²

14 114. The report from Proofpoint was published March 27, 2019, and
15 summarized findings of recent healthcare industry cyber threat surveys and
16 recounted good, common sense steps that the targeted healthcare companies
17 should follow to prevent email-related cyberattacks.

18 115. One of the best protections against email related threats is security
19 awareness training and testing on a regular basis. This should be a key part of a
20 company’s ongoing training of its employees. “[S]ince phishing is still a
21 significant, initial point of compromise, additional work needs to be done to
22 further lower the click rate,” the HIMSS report states. “This can be done through
23 more frequent security awareness training, phishing simulation, and better
24

25
26 ¹¹“Stolen Laptops Lead to Important HIPAA Settlements,” U.S. Dep’t of Health
27 and Human Services (Apr. 22, 2014), available at [https://wayback.archive-
it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-
laptops-lead-to-important-hipaa-settlements.html](https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html).

28 ¹²Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results* (Mar.
27, 2019), [https://www.proofpoint.com/us/security-awareness/post/healthcare-
phishing-statistics-2019-himss-survey-results](https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results).

1 monitoring of metrics pertaining to phishing (including whether there are any
2 particular repeat offenders).”¹³

3 116. ProtonMail Technologies publishes a guide for IT Security to small
4 businesses (i.e., companies without the heightened standard of care applicable in
5 the healthcare industry). In its 2019 guide, ProtonMail dedicates a full chapter of
6 its e-book guide to the danger of phishing and ways to prevent a small business
7 from falling prey to it. It reports:

8 Phishing and fraud are becoming ever more extensive
9 problems. A recent threat survey from the cybersecurity firm
10 Proofpoint stated that between 2017 and 2018, email-based
11 attacks on businesses increased 476 percent. The FBI
12 reported that these types of attacks cost companies around the
13 world \$12 billion annually.

14 Similar to your overall IT security, your email security relies
15 on training your employees to implement security best
16 practices and to recognize possible phishing attempts. This
17 must be deeply ingrained into every staff member so that
18 every time they check their emails, they are alert to the
19 possibility of malicious action.¹⁴

20 117. The guidance that ProtonMail provides non-healthcare industry small
21 businesses is likely still not adequate for companies like MEDNAX and Pediatrix,
22 with the heightened healthcare standard of care based on HIPAA, CMIA, and the
23 increased danger from the sensitivity and wealth of Personal and Medical
24 Information they retain, but ProtonMail’s guidance is informative for showing
25 how inadequately Defendants protected the Personal and Medical Information of
26 the Plaintiffs and the Class. ProofPoint lists numerous tools under the heading,
27 “How to Prevent Phishing”:

28 ¹³*Id.*
¹⁴*The ProtonMail Guide to IT Security for Small Businesses*, PROTONMAIL (2019),
available at <https://protonmail.com/it-security-complete-guide-for-businesses>.

- 1 a. **Training:** “Training your employees on how to
2 recognize phishing emails and what to do when they
3 encounter one is the first and most important step in
4 maintaining email security. *This training should be*
5 *continuous as well. . . .*”
- 6 b. **Limit Public Information:** “Attackers cannot target
7 your employees if they don’t know their email
8 addresses. Don’t publish non-essential contact details
9 on your website or any public directories
- 10 c. **Carefully check emails:** “First off, your employees
11 should be skeptical anytime they receive an email
12 from an unknown sender. Second, most phishing
13 emails are riddled with typos, odd syntax, or stilted
14 language. Finally, check the ‘From’ address to see if
15 it is odd If an email looks suspicious, employees
16 should report it.”
- 17 d. **Beware of links and attachments:** “Do not click on
18 links or download attachments without verifying the
19 source first and establishing the legitimacy of the link
20 or attachment...”
- 21 e. **Do not automatically download remote content:**
22 “Remote content in emails, like photos, can run
23 scripts on your computer that you are not expecting,
24 and advanced hackers can hide malicious code in
25 them. You should configure your email service
26 provider to not automatically download remote
27 content. This will allow you to verify an email is
28

1 legitimate before you run any unknown scripts
2 contained in it.”

3 f. **Hover over hyperlinks:** “Never click on hyperlinked
4 text without hovering your cursor over the link first
5 to check the destination URL, which should appear in
6 the lower corner of your window. Sometimes the
7 hacker might disguise a malicious link as a short
8 URL.” [Proofpoint notes that there are tools online
9 available for retrieving original URLs from shortened
10 ones.]

11 g. **If in doubt, investigate:** “Often phishing emails will
12 try to create a false sense of urgency by saying
13 something requires your immediate action. However,
14 if your employees are not sure if an email is genuine,
15 they should not be afraid to take extra time to verify
16 the email. This might include asking a colleague,
17 your IT security lead, looking up the website of the
18 service the email is purportedly from, or, if they have
19 a phone number, calling the institution, colleague, or
20 client that sent the email.”

21 h. **Take preventative measures:** “Using an end-to-end
22 encrypted email service gives your business’s emails
23 an added layer of protection in the case of a data
24 breach. A spam filter will remove the numerous
25 random emails that you might receive, making it
26 more difficult for a phishing attack to get through.
27 Finally, other tools, like Domain-based Message
28 Authentication, Reporting, and Conformance

1 (DMARC) help you be sure that the email came from
2 the person it claims to come from, making it easier to
3 identify potential phishing attacks.”¹⁵

4 118. As mentioned, these are basic, common-sense email security
5 measures that every business, whether in healthcare or not, should be doing. By
6 adequately taking these common-sense solutions, Defendants could have
7 prevented this Data Breach from occurring.

8 **F. Cyber Criminals Will Use Plaintiffs’ and Class Members’**
9 **Personal and Medical Information to Defraud Them**

10 119. Plaintiffs and Class members’ Personal and Medical Information is of
11 great value to hackers and cyber criminals, and the data stolen in the Data Breach
12 has been used and will continue to be used in a variety of sordid ways for
13 criminals to exploit Plaintiffs and the Class members and to profit off their
14 misfortune.

15 120. Each year, identity theft causes tens of billions of dollars of losses to
16 victims in the United States.¹⁶ For example, with the Personal and Medical
17 Information stolen in the Data Breach, including Social Security numbers, identity
18 thieves can open financial accounts, apply for credit, file fraudulent tax returns,
19 commit crimes, create false driver’s licenses and other forms of identification and
20 sell them to other criminals or undocumented immigrants, steal government
21 benefits, give breach victims’ names to police during arrests, and many other
22 harmful forms of identity theft.¹⁷ These criminal activities have and will result in
23 devastating financial and personal losses to Plaintiffs and the Class members.
24

25 ¹⁵*Id.*

26 ¹⁶“Facts + Statistics: Identity Theft and Cybercrime,” Insurance Info. Inst.,
27 <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>
(discussing Javelin Strategy & Research’s report “2018 Identity Fraud: Fraud
28 Enters a New Era of Complexity”).

¹⁷*See, e.g.,* Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

1 121. Personal and Medical Information is such a valuable commodity to
2 identity thieves that once it has been compromised, criminals will use it and trade
3 the information on the cyber black-market for years.¹⁸

4 122. For example, it is believed that certain Personal and Medical
5 Information compromised in the 2017 Experian data breach was being used, three
6 years later, by identity thieves to apply for COVID-19-related benefits in the state
7 of Oklahoma.¹⁹

8 123. This was a financially motivated Data Breach, as apparent from the
9 discovery of the cyber criminals seeking to profit off of the sale of Plaintiffs' and
10 the Class members' Personal and Medical Information on the dark web. The
11 Personal and Medical Information exposed in this Data Breach are valuable to
12 identity thieves for use in the kinds of criminal activity described herein.

13 124. These risks are both certainly impending and substantial. As the FTC
14 has reported, if hackers get access to personally identifiable information, they will
15 use it.²⁰

16 125. Hackers may not use the information right away. According to the
17 U.S. Government Accountability Office, which conducted a study regarding data
18 breaches:

19 [I]n some cases, stolen data may be held for up to a year or more
20 before being used to commit identity theft. Further, once stolen
21 data have been sold or posted on the Web, fraudulent use of that
22 information may continue for years. As a result, studies that
23 attempt to measure the harm resulting from data breaches cannot
necessarily rule out all future harm.²¹

24 ¹⁸ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007,
25 <https://www.gao.gov/assets/270/262904.html>

26 ¹⁹ See <https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html>; see also <https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/>.

27 ²⁰ Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N
28 (May 24, 2017), <https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

²¹ *Data Breaches Are Frequent*, *supra* note 11.

1 126. For instance, with a stolen Social Security number, which is part of
2 the Personal and Medical Information compromised in the Data Breach, someone
3 can open financial accounts, get medical care, file fraudulent tax returns, commit
4 crimes, and steal benefits.²² Identity thieves can also use the information stolen
5 from Plaintiffs and Class members to qualify for expensive medical care and leave
6 them and their contracted health insurers on the hook for massive medical bills.

7 127. Medical identity theft is one of the most common, most expensive,
8 and most difficult to prevent forms of identity theft. According to Kaiser Health
9 News, “medical-related identity theft accounted for 43 percent of all identity thefts
10 reported in the United States in 2013,” which is more than identity thefts involving
11 banking and finance, the government and the military, or education.²³

12 128. “Medical identity theft is a growing and dangerous crime that leaves
13 its victims with little to no recourse for recovery,” reported Pam Dixon, executive
14 director of World Privacy Forum. “Victims often experience financial
15 repercussions and worse yet, they frequently discover erroneous information has
16 been added to their personal medical files due to the thief’s activities.”²⁴

17 129. As indicated by James Trainor, second in command at the FBI’s
18 cyber security division: “Medical records are a gold mine for criminals—they can
19 access a patient’s name, DOB, Social Security and insurance numbers, and even
20 financial information all in one place. Credit cards can be, say, five dollars or
21 more where [personal health information] can go from \$20 say up to—we’ve seen
22 \$60 or \$70 [(referring to prices on dark web marketplaces)].”²⁵ A complete
23

24 ²² See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social*
25 *Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

26 ²³ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser
27 Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>.

28 ²⁴ *Id.*

²⁵ IDExperts, *You Got It, They Want It: Criminals Targeting Your Private*
Healthcare Data, New Ponemon Study Shows,
<https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat>.

1 identity theft kit that includes health insurance credentials may be worth up to
2 \$1,000 on the black market.²⁶

3 130. If cyber criminals manage to steal financial information, health
4 insurance information, and other personally sensitive data—as they did here—
5 there is no limit to the amount of fraud to which Defendants have exposed the
6 Plaintiffs and Class members.

7 131. A study by Experian found that the average total cost of medical
8 identity theft is “about \$20,000” per incident, and that a majority of victims of
9 medical identity theft were forced to pay out-of-pocket costs for healthcare they
10 did not receive in order to restore coverage.²⁷ Almost half of medical identity
11 theft victims lose their healthcare coverage as a result of the incident, while nearly
12 one-third saw their insurance premiums rise, and forty percent were never able to
13 resolve their identity theft at all.²⁸

14 132. As described above, identity theft victims must spend countless hours
15 and large amounts of money repairing the impact to their credit.²⁹

16 133. The danger of identity theft is compounded when, like here, a minor’s
17 Personal and Medical Information is compromised, because minors typically have
18 no credit reports to monitor. Thus, it can be difficult to monitor because a minor
19 cannot simply place an alert on their credit report or “freeze” their credit report
20 when no credit report exists.

22 ²⁶*Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS:
23 Key findings from The Global State of Information Security Survey 2015,
24 [https://www.pwc.com/gx/en/consulting-services/information-security-](https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf)
25 [survey/assets/the-global-state-of-information-security-survey-2015.pdf](https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf).

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

29 ²⁸ *Id.*; see also *Healthcare Data Breach: What to Know About them and What to*
30 *Do After One*, EXPERIAN, [https://www.experian.com/blogs/ask-](https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/)
31 [experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-](https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/)
32 [one/](https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/).

33 ²⁹ “Guide for Assisting Identity Theft Victims,” Federal Trade Commission, 4
34 (Sept. 2013), [http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-](http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf)
35 [theft-victims.pdf](http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf).

1 134. Defendants’ failure to offer identity monitoring to a majority of the
2 Class, including to Plaintiffs, is egregious. Moreover, Defendants’ offer of one
3 year of identity theft monitoring to only a limited number of Class members
4 (which did not involve Plaintiffs) is, in and of itself, woefully inadequate, as the
5 worst is yet to come.

6 135. With this Data Breach, it is likely that identity thieves have already
7 started to prey on the victims, and one can reasonably anticipate this will continue.

8 136. Victims of the Data Breach, like Plaintiffs and other Class members,
9 must spend many hours and large amounts of money protecting themselves from
10 the current and future negative impacts to their credit because of the Data
11 Breach.³⁰

12 137. In fact, as a direct and proximate result of the Data Breach, Plaintiffs
13 and the Class have been placed at an imminent, immediate, and continuing
14 increased risk of harm from fraud and identity theft. Plaintiffs and the Class must
15 now take the time and effort and spend the money to mitigate the actual and
16 potential impact of the Data Breach on their everyday lives, including purchasing
17 identity theft and credit monitoring services, placing “freezes” and “alerts” with
18 credit reporting agencies, contacting their financial institutions, healthcare
19 providers, closing or modifying financial accounts, and closely reviewing and
20 monitoring bank accounts, credit reports, and health insurance account
21 information for unauthorized activity for years to come.

22 138. Plaintiffs and the Class have suffered, and continue to suffer, actual
23 harms for which they are entitled to compensation, including:

- 24 a. Trespass, damage to, and theft of their personal property
25 including Personal and Medical Information;
26 b. Improper disclosure of their Personal and Medical Information;

27 _____
28 ³⁰ “Guide for Assisting Identity Theft Victims,” Federal Trade Commission, 4
(Sept. 2013), <http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf>.

- 1 c. The imminent and certainly impending injury flowing from
- 2 potential fraud and identity theft posed by their Personal and
- 3 Medical Information being placed in the hands of criminals
- 4 and having been already misused;
- 5 d. The imminent and certainly impending risk of having their
- 6 confidential medical information used against them by spam
- 7 callers to defraud them;
- 8 e. Damages flowing from Defendants untimely and inadequate
- 9 notification of the data breach;
- 10 f. Loss of privacy suffered as a result of the Data Breach;
- 11 g. Ascertainable losses in the form of out-of-pocket expenses and
- 12 the value of their time reasonably expended to remedy or
- 13 mitigate the effects of the data breach;
- 14 h. Ascertainable losses in the form of deprivation of the value of
- 15 patients' personal information for which there is a well-
- 16 established and quantifiable national and international market;
- 17 i. The loss of use of and access to their credit, accounts, and/or
- 18 funds;
- 19 j. Damage to their credit due to fraudulent use of their Personal
- 20 and Medical Information; and
- 21 k. Increased cost of borrowing, insurance, deposits and other
- 22 items which are adversely affected by a reduced credit score.

23 139. Moreover, Plaintiffs and Class members have an interest in ensuring
24 that their information, which remains in the possession of Defendants, is protected
25 from further breaches by the implementation of industry standard and statutorily
26 compliant security measures and safeguards. Defendants have shown themselves
27 to be wholly incapable of protecting Plaintiffs' and Class members' Personal and
28 Medical Information.

1 140. Plaintiffs and Class members are desperately trying to mitigate the
2 damage that Defendants have caused them but, given the kind of Personal and
3 Medical Information Defendants made accessible to hackers, they are certain to
4 incur additional damages. Because identity thieves have their Personal and
5 Medical Information, Plaintiffs and all Class members will need to have identity
6 theft monitoring protection for the rest of their lives. Some, including babies and
7 young children, may even need to go through the long and arduous process of
8 getting a new Social Security number, with all the loss of credit and employment
9 difficulties that come with this change.³¹

10 141. None of this should have happened. The Data Breach was
11 preventable.

12 **G. Defendants Could Have Prevented the Data Breach but Failed**
13 **to Adequately Protect Plaintiffs’ and Class Members’ Personal**
14 **and Medical Information**

15 142. Data breaches are preventable.³² As Lucy Thompson wrote in the
16 DATA BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data
17 breaches that occurred could have been prevented by proper planning and the
18 correct design and implementation of appropriate security solutions.”³³ She added
19 that “[o]rganizations that collect, use, store, and share sensitive personal data must
20 accept responsibility for protecting the information and ensuring that it is not
21 compromised”³⁴

22 143. “Most of the reported data breaches are a result of lax security and
23 the failure to create or enforce appropriate security policies, rules, and procedures
24 ... Appropriate information security controls, including encryption, must be

25 ³¹*Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov.
26 16, 2015), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html>.

27 ³²Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are
28 Preventable,” *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson,
ed., 2012)

³³*Id.* at 17.

³⁴*Id.* at 28.

1 implemented and enforced in a rigorous and disciplined manner so that a *data*
2 *breach never occurs.*”³⁵

3 144. Defendants required Plaintiffs and Class members to surrender their
4 Personal and Medical Information – including but not limited to their names,
5 addresses, Social Security numbers, medical information, and health insurance
6 information – and were entrusted with properly holding, safeguarding, and
7 protecting against unlawful disclosure of such Personal and Medical Information.

8 145. Many failures laid the groundwork for the success (“success” from a
9 cybercriminal’s viewpoint) of the Data Breach, starting with Defendants’ failure
10 to incur the costs necessary to implement adequate and reasonable cyber security
11 procedures and protocols necessary to protect Plaintiffs’ and Class members’
12 Personal and Medical Information.

13 146. Defendants maintained the Personal and Medical Information in a
14 reckless manner. In particular, the Personal and Medical Information was
15 maintained and/or exchanged, unencrypted, in Microsoft Office 365 business
16 email accounts that were maintained in a condition vulnerable to cyberattacks.

17 147. Defendants knew, or reasonably should have known, of the
18 importance of safeguarding Personal and Medical Information and of the
19 foreseeable consequences that would occur if Plaintiffs’ and Class members’
20 Personal and Medical Information was stolen, including the significant costs that
21 would be placed on Plaintiffs and Class members as a result of a breach.

22 148. The mechanism of the cyberattack and potential for improper
23 disclosure of Plaintiffs’ and Class members’ Personal and Medical Information
24 was a known risk to Defendants, and thus Defendants were on notice that failing
25 to take necessary steps to secure Plaintiffs’ and Class members’ Personal and
26 Medical Information from those risks left that information in a dangerous
27 condition.

28 _____
³⁵*Id.*

1 149. Defendants disregarded the rights of Plaintiffs and Class members by,
2 *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take
3 adequate and reasonable measures to ensure that their business email accounts
4 were protected against unauthorized intrusions; (ii) failing to disclose that they did
5 not have adequately robust security protocols and training practices in place to
6 adequately safeguard Plaintiffs' and Class members' Personal and Medical
7 Information; (iii) failing to take standard and reasonably available steps to prevent
8 the Data Breach; (iv) concealing the existence and extent of the Data Breach for
9 an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class
10 members prompt and accurate notice of the Data Breach.

11 **V. CLASS ACTION ALLEGATIONS**

12 150. Plaintiffs incorporate by reference all allegations of the preceding
13 paragraphs as though fully set forth herein.

14 151. Plaintiffs bring all claims as class claims under Federal Rule of Civil
15 Procedure 23. Plaintiffs asserts all claims on behalf of the Nationwide Class,
16 defined as follows:

17 **All persons residing in the United States whose personal and**
18 **medical information was compromised as a result of the**
19 **MEDNAX and Pediatrix Data Breach that occurred in June**
20 **2020.**

21 152. Alternatively, Plaintiffs propose the following alternative classes by
22 state, as follows:

23 **[Name of State] Subclass: All residents of [name of State]**
24 **whose personal and medical information was compromised**
25 **as a result of the MEDNAX and Pediatrix Data Breach that**
26 **occurred in June 2020.**

27 153. Also, in the alternative, Plaintiffs request additional subclasses as
28 necessary based on the types of Personal and Medical Information that were
compromised.

1 154. Excluded from the Nationwide Class and Subclasses are Defendants,
2 any entity in which Defendants have a controlling interest, and Defendants’
3 officers, directors, legal representatives, successors, subsidiaries, and assigns. Also
4 excluded from the Class is any judge, justice, or judicial officer presiding over this
5 matter and members of their immediate families and judicial staff.

6 155. Plaintiffs reserve the right to amend the above definitions or to
7 propose alternative or additional subclasses in subsequent pleadings and motions
8 for class certification.

9 156. The proposed Nationwide Class or, alternatively, the separate
10 Statewide Subclasses (collectively referred to herein as the “Class” unless
11 otherwise specified) meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2),
12 (b)(3), and (c)(4).

13 157. **Numerosity:** The proposed Class is believed to be so numerous that
14 joinder of all members is impracticable. The proposed Subclass is also believed to
15 be so numerous that joinder of all members would be impractical.

16 158. **Typicality:** Plaintiffs’ claims are typical of the claims of the Class.
17 Plaintiffs and all members of the Class were injured through Defendants’ uniform
18 misconduct. The same event and conduct that gave rise to Plaintiffs’ claims are
19 identical to those that give rise to the claims of every other Class member because
20 Plaintiffs and each member of the Class had their sensitive Personal and Medical
21 Information compromised in the same way by the same conduct of Defendants.

22 159. **Adequacy:** Plaintiffs are adequate representatives of the Class
23 because their interests do not conflict with the interests of the Class and proposed
24 Subclasses that they seek to represent; Plaintiffs have retained counsel competent
25 and highly experienced in data breach class action litigation; and Plaintiffs and
26 Plaintiffs’ counsel intend to prosecute this action vigorously. The interests of the
27 Class will be fairly and adequately protected by Plaintiffs and their counsel.
28

1 160. **Superiority:** A class action is superior to other available means of
2 fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury
3 suffered by each individual Class member is relatively small in comparison to the
4 burden and expense of individual prosecution of complex and expensive litigation.
5 It would be very difficult, if not impossible, for members of the Class individually
6 to effectively redress Defendants’ wrongdoing. Even if Class members could
7 afford such individual litigation, the court system could not. Individualized
8 litigation presents a potential for inconsistent or contradictory judgments.
9 Individualized litigation increases the delay and expense to all parties, and to the
10 court system, presented by the complex legal and factual issues of the case. By
11 contrast, the class action device presents far fewer management difficulties and
12 provides benefits of single adjudication, economy of scale, and comprehensive
13 supervision by a single court.

14 161. **Commonality and Predominance:** There are many questions of law
15 and fact common to the claims of Plaintiffs and the other members of the Class,
16 and those questions predominate over any questions that may affect individual
17 members of the Class. Common questions for the Class include:

- 18 a. Whether Defendants engaged in the wrongful conduct alleged
19 herein;
- 20 b. Whether Defendants failed to adequately safeguard Plaintiffs’
21 and the Class’s Personal and Medical Information;
- 22 c. Whether Defendants’ email and computer systems and data
23 security practices used to protect Plaintiffs’ and Class members’
24 Personal and Medical Information violated the FTC Act,
25 HIPAA, CMIA, and/or state laws and/or Defendants’ other
26 duties discussed herein;

- 1 d. Whether Defendants owed a duty to Plaintiffs and the Class to
- 2 adequately protect their Personal and Medical Information, and
- 3 whether they breached this duty;
- 4 e. Whether Defendants knew or should have known that their
- 5 computer and network security systems and business email
- 6 accounts were vulnerable to a data breach;
- 7 f. Whether Defendants' conduct, including their failure to act,
- 8 resulted in or was the proximate cause of the Data Breach;
- 9 g. Whether Defendants breached contractual duties to Plaintiffs
- 10 and the Class to use reasonable care in protecting their Personal
- 11 and Medical Information;
- 12 h. Whether Defendants failed to adequately respond to the Data
- 13 Breach, including failing to investigate it diligently and notify
- 14 affected individuals in the most expedient time possible and
- 15 without unreasonable delay, and whether this caused damages
- 16 to Plaintiffs and the Class;
- 17 i. Whether Defendants continue to breach duties to Plaintiffs and
- 18 the Class;
- 19 j. Whether Plaintiffs and the Class suffered injury as a proximate
- 20 result of Defendants' negligent actions or failures to act;
- 21 k. Whether Plaintiffs and the Class are entitled to recover damages,
- 22 equitable relief, and other relief;
- 23 l. Whether injunctive relief is appropriate and, if so, what
- 24 injunctive relief is necessary to redress the imminent and
- 25 currently ongoing harm faced by Plaintiffs and members of the
- 26 Class and the general public;
- 27 m. Whether Defendants' actions alleged herein constitute gross
- 28 negligence; and

1 n. Whether Plaintiffs and Class members are entitled to punitive
2 damages.

3 **VI. CAUSES OF ACTION**

4 **A. COUNT I – NEGLIGENCE**

5 162. Plaintiffs incorporate by reference all allegations of the preceding
6 paragraphs as though fully set forth herein.

7 163. Defendants solicited, gathered, and stored the Personal and Medical
8 Information of Plaintiffs and the Class as part of the operation of their business.

9 164. Upon accepting and storing the Personal and Medical Information of
10 Plaintiffs and Class members, Defendants undertook and owed a duty to Plaintiffs
11 and Class members to exercise reasonable care to secure and safeguard that
12 information and to use secure methods to do so.

13 165. Defendants had full knowledge of the sensitivity of the Personal and
14 Medical Information, the types of harm that Plaintiffs and Class members could
15 and would suffer if the Personal and Medical Information was wrongfully
16 disclosed, and the importance of adequate security.

17 166. Plaintiffs and Class members were the foreseeable victims of any
18 inadequate safety and security practices. Plaintiffs and the Class members had no
19 ability to protect their Personal and Medical Information that was in Defendants'
20 possession. As such, a special relationship existed between Defendants and
21 Plaintiffs and the Class.

22 167. Defendants were well aware of the fact that cyber criminals routinely
23 target large corporations through cyberattacks in an attempt to steal sensitive
24 personal and medical information.

25 168. Defendants owed Plaintiffs and the Class members a common law
26 duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs
27 and the Class when obtaining, storing, using, and managing personal information,
28 including taking action to reasonably safeguard such data and providing

1 notification to Plaintiffs and the Class members of any breach in a timely manner
2 so that appropriate action could be taken to minimize losses.

3 169. Defendants' duty extended to protecting Plaintiffs and the Class from
4 the risk of foreseeable criminal conduct of third parties, which has been
5 recognized in situations where the actor's own conduct or misconduct exposes
6 another to the risk or defeats protections put in place to guard against the risk, or
7 where the parties are in a special relationship. *See* Restatement (Second) of Torts
8 § 302B. Numerous courts and legislatures also have recognized the existence of a
9 specific duty to reasonably safeguard personal information.

10 170. Defendants had duties to protect and safeguard the Personal and
11 Medical Information of Plaintiffs and the Class from being vulnerable to
12 cyberattacks by taking common-sense precautions when dealing with sensitive
13 Personal and Medical Information. Additional duties that Defendants owed
14 Plaintiffs and the Class include:

- 15 a. To exercise reasonable care in designing, implementing,
16 maintaining, monitoring, and testing Defendants' networks,
17 systems, protocols, policies, procedures and practices to ensure
18 that Plaintiffs' and Class members' Personal and Medical
19 Information was adequately secured from impermissible
20 release, disclosure, and publication;
- 21 b. To protect Plaintiffs' and Class members' Personal and
22 Medical Information in their possession by using reasonable
23 and adequate security procedures and systems;
- 24 c. To implement processes to quickly detect a data breach,
25 security incident, or intrusion involving their business email
26 system, networks and servers; and

- 1 d. To promptly notify Plaintiffs and Class members of any data
2 breach, security incident, or intrusion that affected or may have
3 affected their Personal and Medical Information.

4 171. Only Defendants were in a position to ensure that their systems and
5 protocols were sufficient to protect the Personal and Medical Information that
6 Plaintiffs and the Class had entrusted to them.

7 172. Defendants breached their duties of care by failing to adequately
8 protect Plaintiffs' and Class members' Personal and Medical Information.

9 Defendants breached their duties by, among other things:

- 10 a. Failing to exercise reasonable care in obtaining, retaining
11 securing, safeguarding, deleting, and protecting the Personal
12 and Medical Information in their possession;
- 13 b. Failing to protect the Personal and Medical Information in their
14 possession using reasonable and adequate security procedures
15 and systems;
- 16 c. Failing to adequately and properly audit, test, and train their
17 employees to avoid phishing emails;
- 18 d. Failing to use adequate email security systems, including
19 healthcare industry standard SPAM filters, DMARC
20 enforcement, and/or Sender Policy Framework enforcement to
21 protect against phishing emails;
- 22 e. Failing to adequately and properly audit, test, and train their
23 employees regarding how to properly and securely transmit
24 and store Personal and Medical Information;
- 25 f. Failing to adequately train their employees to not store
26 Personal and Medical Information in their email inboxes longer
27 than absolutely necessary for the specific purpose that it was
28 sent or received;

- 1 g. Failing to consistently enforce security policies aimed at
- 2 protecting Plaintiffs' and the Class's Personal and Medical
- 3 Information;
- 4 h. Failing to implement processes to quickly detect data breaches,
- 5 security incidents, or intrusions;
- 6 i. Failing to promptly notify Plaintiffs and Class members of the
- 7 Data Breach that affected their Personal and Medical
- 8 Information.

9 173. Defendants' willful failure to abide by these duties was wrongful,
10 reckless, and grossly negligent in light of the foreseeable risks and known threats.

11 174. As a proximate and foreseeable result of Defendants' grossly
12 negligent conduct, Plaintiffs and the Class have suffered damages and are at
13 imminent risk of additional harms and damages (as alleged above).

14 175. Through Defendants' acts and omissions described herein, including
15 but not limited to Defendants' failure to protect the Personal and Medical
16 Information of Plaintiffs and Class members from being stolen and misused,
17 Defendants unlawfully breached their duty to use reasonable care to adequately
18 protect and secure the Personal and Medical Information of Plaintiffs and Class
19 members while it was within Defendants' possession and control.

20 176. Further, through their failure to provide timely and clear notification
21 of the Data Breach to Plaintiffs and Class members, Defendants prevented
22 Plaintiffs and Class members from taking meaningful, proactive steps to securing
23 their Personal and Medical Information and mitigating damages.

24 177. As a result of the Data Breach, Plaintiffs and Class members have
25 spent time, effort, and money to mitigate the actual and potential impact of the
26 Data Breach on their lives, including but not limited to, paying for credit
27 monitoring and identity theft prevention services that, in most cases, were not
28 offered to them by Defendants, and closely reviewing and monitoring bank

1 accounts, credit reports, and statements sent from providers and their insurance
2 companies.

3 178. Defendants’ wrongful actions, inactions, and omissions constituted
4 (and continue to constitute) common law negligence.

5 179. The damages Plaintiffs and the Class have suffered (as alleged above)
6 and will suffer were and are the direct and proximate result of Defendants’ grossly
7 negligent conduct.

8 180. In addition to its duties under common law, Defendants had
9 additional duties imposed by statute and regulations, including the duties under
10 HIPAA, the FTC Act, the CCRA, and the CMIA. The harms which occurred as a
11 result of Defendants’ failure to observe these duties, including the loss of privacy,
12 significant risk of identity theft, and Plaintiffs’ overpayment for goods and
13 services, are the types of harm that these statutes and their regulations were
14 intended to prevent.

15 181. Defendants violated these statutes when they engaged in the actions
16 and omissions alleged herein and Plaintiffs’ injuries were a direct and proximate
17 result of Defendants’ violations of these statutes. Plaintiffs therefore are entitled to
18 the evidentiary presumptions for negligence *per se* under Cal. Evid. Code § 669.

19 182. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendants owed a duty
20 to Plaintiffs and the Class to provide fair and adequate computer systems and data
21 security to safeguard the Personal and Medical Information of Plaintiffs and the
22 Class.

23 183. Defendants are entities covered by HIPAA, 45 C.F.R. §160.102, and
24 as such are required to comply with HIPAA’s Privacy Rule and Security Rule.
25 HIPAA requires Defendants to “reasonably protect” confidential data from “any
26 intentional or unintentional use or disclosure” and to “have in place appropriate
27 administrative, technical, and physical safeguards to protect the privacy of
28 protected health information.” 45 C.F.R. § 164.530(c)(1). HIPAA also requires

1 Defendants to obtain satisfactory assurances that their business associates would
2 appropriately safeguard the protected health information they receive or create on
3 behalf of the Defendants. 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and
4 (e). The confidential data at issue in this case constitutes “protected health
5 information” within the meaning of HIPAA.

6 184. HIPAA further requires Defendants to disclose the unauthorized
7 access and theft of the protected health information of Plaintiffs and the Class
8 “without unreasonable delay” so that Plaintiffs and Class members could take
9 appropriate measures to mitigate damages, protect against adverse consequences,
10 and thwart future misuse of their personal information. *See* 45 C.F.R. §§ 164.404,
11 164.406, and 164.410.

12 185. The FTC Act prohibits “unfair practices in or affecting commerce,”
13 including, as interpreted and enforced by the FTC, the unfair act or practice by
14 businesses, such as Defendants, of failing to use reasonable measures to protect
15 Personal and Medical Information. The FTC publications and orders described
16 above also formed part of the basis of Defendants’ duty in this regard.

17 186. Defendants gathered and stored the Personal and Medical
18 Information of Plaintiffs and the Class as part of their business of soliciting their
19 services to their patients, which solicitations and services affect commerce.

20 187. Defendants violated the FTC Act by failing to use reasonable
21 measures to protect the Personal and Medical Information of Plaintiffs and the
22 Class and by not complying with applicable industry standards, as described
23 herein.

24 188. Defendants breached their duties to Plaintiffs and the Class under the
25 FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer
26 systems and/or data security practices to safeguard Plaintiffs’ and Class members’
27 Personal and Medical Information, and by failing to provide prompt notice
28 without reasonable delay.

1 189. Defendants' failure to comply with applicable laws and regulations
2 constitutes negligence *per se*.

3 190. Plaintiffs and the Class are within the class of persons that HIPAA
4 and the FTC Act were intended to protect.

5 191. The harm that occurred as a result of the Data Breach is the type of
6 harm the FTC Act and HIPAA were intended to guard against.

7 192. Defendants breached their duties to Plaintiffs and the Class under
8 these laws by failing to provide fair, reasonable, or adequate computer systems
9 and data security practices to safeguard Plaintiffs' and the Class's Personal and
10 Medical Information.

11 193. Additionally, Defendants had a duty to promptly notify victims of the
12 Data Breach. For instance, HIPAA required Defendants to notify victims of the
13 Breach within sixty (60) days of the discovery of the Data Breach. Defendants did
14 not notify Plaintiffs or Class members of the Data Breach until around December
15 16, 2020.

16 194. Defendants knew on or before June 17, 2020, that unauthorized
17 persons had accessed and/or viewed or were reasonably likely to have accessed
18 and/or viewed private, protected, personal information of Plaintiffs and the Class.

19 195. Defendants breached their duties to Plaintiffs and the Class by
20 unreasonably delaying and failing to provide notice expeditiously and/or as soon
21 as practicable to Plaintiffs and the Class of the Data Breach.

22 196. Defendants' violation of the FTC Act and HIPAA constitutes
23 negligence *per se*.

24 197. As a direct and proximate result of Defendants' negligence *per se*,
25 Plaintiffs and the Class have suffered, and continue to suffer, damages arising
26 from the Data Breach, as alleged above.
27
28

1 198. The injury and harm that Plaintiffs and Class members suffered (as
2 alleged above) was the direct and proximate result of Defendants’ negligence *per*
3 *se*.

4 199. Plaintiffs and the Class have suffered injury and are entitled to actual
5 and punitive damages in amounts to be proven at trial.

6 **B. COUNT II – INVASION OF PRIVACY**

7 200. Plaintiffs incorporates by reference all allegations of the preceding
8 paragraphs as though fully set forth herein.

9 201. California established the right to privacy in Article 1, Section 1 of
10 the California Constitution.

11 202. The State of California recognizes the tort of Intrusion into Private
12 Affairs and adopts the formulation of that tort found in the Restatement (Second)
13 of Torts, which states, “One who intentionally intrudes, physically or otherwise,
14 upon the solitude or seclusion of another or his private affairs or concerns is
15 subject to liability to the other for invasion of his privacy if the intrusion would be
16 highly offensive to a reasonable person.” Restatement (Second) of Torts, § 652B
17 (1977).

18 203. The states of Oklahoma, Washington, and Texas also recognize the
19 tort of Invasion of Privacy and, like California, adopt the formulation of that tort
20 found in the Restatement (Second) of Torts.

21 204. Plaintiffs and Class members had a legitimate and reasonable
22 expectation of privacy with respect to their Personal and Medical Information and
23 were accordingly entitled to the protection of this information against disclosure to
24 and acquisition by unauthorized third parties.

25 205. Defendants owed a duty to its patients, including Plaintiffs and Class
26 members, to keep their Personal and Medical Information confidential.

27 206. The unauthorized access, acquisition, appropriation, disclosure,
28 encumbrance, exfiltration, release, theft, use, and/or viewing of Personal and

1 Medical Information, especially the type of information that is the subject of this
2 action, is highly offensive to a reasonable person.

3 207. The intrusion was into a place or thing that was private and is entitled
4 to be private. Plaintiffs and Class members disclosed their Personal and Medical
5 Information to Defendants as part of their receiving medical care and treatment
6 from Defendants, but privately, with the intention that such highly sensitive
7 information would be kept confidential and protected from unauthorized access,
8 acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft,
9 use, and/or viewing. Plaintiffs and Class members were reasonable in their belief
10 that such information would be kept private and would not be disclosed without
11 their authorization.

12 208. The Data Breach constitutes an intentional interference with
13 Plaintiffs' and Class members' interest in solitude or seclusion, either as to their
14 persons or as to their private affairs or concerns, of a kind that would be highly
15 offensive to a reasonable person.

16 209. Defendants acted with a knowing state of mind when they permitted
17 the Data Breach because they knew their information security practices were
18 inadequate.

19 210. Acting with knowledge, Defendants had notice and knew that their
20 inadequate cybersecurity practices would cause injury to Plaintiffs and Class
21 members.

22 211. As a proximate result of Defendants' acts and omissions, Plaintiffs'
23 and Class members' Personal and Medical Information was accessed by, acquired
24 by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to,
25 stolen by, used by, and/ or reviewed by third parties without authorization, causing
26 Plaintiffs and Class members to suffer damages.

27 212. Unless and until enjoined and restrained by order of this Court,
28 Defendants' wrongful conduct will continue to cause great and irreparable injury

1 to Plaintiffs and Class members in that the Personal and Medical Information
2 maintained by Defendants can be accessed by, acquired by, appropriated by,
3 disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/ or
4 viewed by unauthorized persons.

5 213. Plaintiffs and the Class have no adequate remedy at law for the
6 injuries in that a judgment for monetary damages will not end the invasion of
7 privacy for Plaintiffs and Class members.

8 **C. COUNT III – UNJUST ENRICHMENT**

9 214. Plaintiffs incorporate by reference all allegations of the preceding
10 paragraphs as though fully set forth herein.

11 215. Plaintiffs and the Class bring this claim in the alternative to all other
12 claims and remedies at law.

13 216. Plaintiffs and Class members conferred a monetary benefit upon
14 Defendants in the form of monetary payments to obtain medical services from
15 Defendants.

16 217. Defendants collected, maintained, and stored the Personal and
17 Medical Information of Plaintiffs and Class members and, as such, Defendants
18 had direct knowledge of the monetary benefits conferred upon them by Plaintiffs
19 and Class members.

20 218. Defendants, by way of their affirmative actions and omissions,
21 including their knowing violations of their express or implied contracts with
22 Plaintiffs and the Class members, knowingly and deliberately enriched themselves
23 by saving the costs they reasonably and contractually should have expended on
24 HIPAA and CMIA compliance and reasonable data privacy and security measures
25 to secure Plaintiffs' and Class members' Personal and Medical Information.

26 219. Instead of providing a reasonable level of security, training, and
27 protocols that would have prevented the Data Breach, as described above and as is
28 common industry practice among companies entrusted with similar Personal and

1 Medical Information, Defendants, upon information and belief, instead
2 consciously and opportunistically calculated to increase their own profits at the
3 expense of Plaintiffs and Class members (and continue to do so by electing to not
4 provide free credit monitoring services to a majority of Class members negatively
5 impacted by the Data Breach).

6 220. As a direct and proximate result of Defendants' decision to profit
7 rather than provide adequate data security, Plaintiffs and Class members suffered
8 and continue to suffer actual damages in (i) the amount of the savings and costs
9 Defendants reasonably and contractually should have expended on data security
10 measures to secure Plaintiffs' Personal and Medical Information, (ii) time and
11 expenses mitigating harms, (iii) diminished value of Personal and Medical
12 Information, (iv) loss of privacy, and (v) an increased risk of future identity theft.

13 221. Defendants, upon information and belief, have therefore engaged in
14 opportunistic, unethical, and immoral conduct by profiting from conduct that they
15 knew would create a significant and highly likely risk of substantial and certainly
16 impending harm to Plaintiffs and the Class in direct violation of Plaintiffs' and
17 Class members' legally protected interests. As such, it would be inequitable,
18 unconscionable, and unlawful to permit Defendants to retain the benefits they
19 derived as a consequence of their breach.

20 222. Accordingly, Plaintiffs and the Class are entitled to relief in the form
21 of restitution and disgorgement of all ill-gotten gains, which should be put into a
22 common fund to be distributed to Plaintiffs and the Class.

23 **D. COUNT IV – BREACH OF CONTRACT**

24 223. Plaintiffs incorporate by reference all allegations of the preceding
25 paragraphs as though fully set forth herein.

26 224. Plaintiffs and the Class entered into contracts with Defendants and
27 provided payment to Defendants in exchange for Defendants' provision of
28 medical services.

1 225. The promises and representations described above relating to
2 compliance with HIPAA, CMIA and industry practices, and about Defendants’
3 concern for their patients’ privacy rights, became terms of the contract between
4 them and their patients, including Plaintiffs and the Class.

5 226. Defendants breached these promises by failing to comply with
6 HIPAA, CMIA, and reasonable industry practices.

7 227. As a result of Defendants’ breach of these terms, Plaintiffs and the
8 Class have been seriously harmed and put at grave risk of debilitating future
9 harms.

10 228. Plaintiffs and Class members are therefore entitled to damages in an
11 amount to be determined at trial.

12 **E. COUNT V – BREACH OF IMPLIED CONTRACT**
13 **(ALTERNATIVELY TO COUNT IV)**

14 229. Plaintiffs incorporate by reference all allegations of the preceding
15 paragraphs as though fully set forth herein.

16 230. When Plaintiffs and the Class members provided their Personal and
17 Medical Information to Defendants when seeking medical services, they entered
18 into implied contracts in which Defendants agreed to comply with their statutory
19 and common law duties to protect Plaintiffs’ and Class members’ Personal and
20 Medical Information and to timely notify them in the event of a data breach.

21 231. Defendants required their patients to provide Personal and Medical
22 Information in order to receive medical services from their affiliate doctors and
23 clinicians.

24 232. Defendants affirmatively represented that they collected and stored
25 the Personal and Medical Information of Plaintiffs and the members of the Class
26 in compliance with HIPAA, the CMIA, and other statutory and common law
27 duties, and using reasonable, industry standard means.
28

1 233. Based on the implicit understanding and also on Defendants’
2 representations (as described above), Plaintiffs and the Class accepted Defendants’
3 offers and provided Defendants with their Personal and Medical Information.

4 234. Plaintiffs and Class members would not have provided their Personal
5 and Medical Information to Defendants had they known that Defendants would
6 not safeguard their Personal and Medical Information, as promised, or provide
7 timely notice of a data breach.

8 235. Plaintiffs and Class members fully performed their obligations under
9 the implied contracts with Defendants.

10 236. Defendants breached the implied contracts by failing to safeguard
11 Plaintiffs’ and Class members’ Personal and Medical Information and by failing to
12 provide them with timely and accurate notice of the Data Breach.

13 237. The losses and damages Plaintiffs and Class members sustained (as
14 described above) were the direct and proximate result of Defendants’ breach of the
15 implied contract with Plaintiffs and Class members.

16 **F. COUNT VI – BREACH OF CONFIDENCE**

17 238. Plaintiffs incorporate by reference all allegations of the preceding
18 paragraphs as though fully set forth herein.

19 239. At all times during Plaintiffs’ and Class members’ interactions with
20 Defendants, Defendants were fully aware of the confidential nature of the Personal
21 and Medical Information that Plaintiffs and Class members provided to
22 Defendants.

23 240. As alleged herein and above, Defendants’ relationship with Plaintiffs
24 and the Class was governed by promises and expectations that Plaintiffs and Class
25 members’ Personal and Medical Information would be collected, stored, and
26 protected in confidence, and would not be accessed by, acquired by, appropriated
27 by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by,
28 and/or viewed by unauthorized third parties.

1 241. Plaintiffs and Class members provided their respective Personal and
2 Medical Information to Defendants with the explicit and implicit understandings
3 that Defendants would protect and not permit the Personal and Medical
4 Information to be accessed by, acquired by, appropriated by, disclosed to,
5 encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by
6 unauthorized third parties.

7 242. Plaintiffs and Class members also provided their Personal and
8 Medical Information to Defendants with the explicit and implicit understandings
9 that Defendants would take precautions to protect their Personal and Medical
10 Information from unauthorized access, acquisition, appropriation, disclosure,
11 encumbrance, exfiltration, release, theft, use, and/or viewing, such as following
12 basic principles of protecting their networks, data systems, and employee business
13 email accounts.

14 243. Defendants voluntarily received, in confidence, Plaintiffs' and Class
15 members' Personal and Medical Information with the understanding that the
16 Personal and Medical Information would not be accessed by, acquired by,
17 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen
18 by, used by, and/or viewed by the public or any unauthorized third parties.

19 244. Due to Defendants' failure to prevent, detect, and avoid the Data
20 Breach from occurring by, inter alia, not following best information security
21 practices to secure Plaintiffs' and Class members' Personal and Medical
22 Information, Plaintiffs' and Class members' Personal and Medical Information
23 was accessed by, acquired by, appropriated by, disclosed to, encumbered by,
24 exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third
25 parties beyond Plaintiffs' and Class members' confidence, and without their
26 express permission.

27 245. As a direct and proximate cause of Defendants' actions and/or
28 omissions, Plaintiffs and Class members have suffered damages as alleged herein.

1 246. But for Defendants’ failure to maintain and protect Plaintiffs’ and
2 Class members’ Personal and Medical Information in violation of the parties’
3 understanding of confidence, their Personal and Medical Information would not
4 have been accessed by, acquired by, appropriated by, disclosed to, encumbered by,
5 exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third
6 parties. Defendants’ Data Breach was the direct and legal cause of the misuse of
7 Plaintiffs’ and Class members’ Personal and Medical Information, as well as the
8 resulting damages.

9 247. The injury and harm Plaintiffs and Class members suffered and will
10 continue to suffer was the reasonably foreseeable result of Defendants’
11 unauthorized misuse of Plaintiffs’ and Class members’ Personal and Medical
12 Information. Defendants knew their data systems and protocols for accepting and
13 securing Plaintiffs’ and Class members’ Personal and Medical Information had
14 security and other vulnerabilities that placed Plaintiffs’ and Class members’
15 Personal and Medical Information in jeopardy.

16 248. As a direct and proximate result of Defendants’ breaches of
17 confidence, Plaintiffs and Class members have suffered and will suffer injury, as
18 alleged herein, including but not limited to (a) actual identity theft; (b) the
19 compromise, publication, and/or theft of their Personal and Medical Information;
20 (c) out-of-pocket expenses associated with the prevention, detection, and recovery
21 from identity theft and/or unauthorized use of their Personal and Medical
22 Information; (d) lost opportunity costs associated with effort expended and the
23 loss of productivity addressing and attempting to mitigate the actual and future
24 consequences of the Data Breach, including but not limited to efforts spent
25 researching how to prevent, detect, contest, and recover from identity theft; (e) the
26 continued risk to their Personal and Medical Information, which remains in
27 Defendants’ possession and is subject to further unauthorized disclosures so long
28 as Defendants fail to undertake appropriate and adequate measures to protect

1 Class Members' Personal and Medical Information in their continued possession;
2 (f) future costs in terms of time, effort, and money that will be expended as result
3 of the Data Breach for the remainder of the lives of Plaintiffs and Class Members;
4 and (g) the diminished value of Defendants' services Plaintiffs and Class members
5 received.

6 **G. COUNT VII – BREACH OF IMPLIED COVENANT OF**
7 **GOOD FAITH AND FAIR DEALING**

8 249. Plaintiffs incorporate by reference all allegations of the preceding
9 paragraphs as though fully set forth herein.

10 250. As described above, Defendants made promises and representations
11 to Plaintiffs and the Class that they would comply with HIPAA and other
12 applicable laws and industry best practices.

13 251. These promises and representations became a part of the contract
14 between Defendants and Plaintiffs and the Class.

15 252. While Defendants had discretion in the specifics of how they met the
16 applicable laws and industry standards, this discretion was governed by an implied
17 covenant of good faith and fair dealing.

18 253. Defendants breached this implied covenant when they engaged in
19 acts and/or omissions that are declared unfair trade practices by the FTC and state
20 statutes and regulations (including California's and Oklahoma's UCL), and when
21 they engaged in unlawful practices under HIPAA, the CMIA, and other state
22 personal and medical privacy laws. These acts and omissions included:
23 representing that they would maintain adequate data privacy and security practices
24 and procedures to safeguard the Personal and Medical Information from
25 unauthorized disclosures, releases, data breaches, and theft; omitting, suppressing,
26 and concealing the material fact of the inadequacy of the privacy and security
27 protections for the Class's Personal and Medical Information; and failing to
28 disclose to the Class at the time they provided their Personal and Medical

1 Information to them that Defendants’ data security systems and protocols,
2 including training, auditing, and testing of employees, failed to meet applicable
3 legal and industry standards.

4 254. Plaintiffs and Class members did all or substantially all the
5 significant things that the contract required them to do.

6 255. Likewise, all conditions required for Defendants’ performance were
7 met.

8 256. Defendants’ acts and omissions unfairly interfered with Plaintiffs’
9 and Class members’ rights to receive the full benefit of their contracts.

10 257. Plaintiffs and Class members have been harmed by Defendants’
11 breach of this implied covenant in the many ways described above, including
12 overpayment for services, the purchase of identity theft monitoring services not
13 provided by Defendants, imminent risk of certainly impending and devastating
14 identity theft that exists now that cyber criminals have their Personal and Medical
15 Information, and the attendant long-term time and expenses spent attempting to
16 mitigate and insure against these risks.

17 258. Defendants are liable for this breach of these implied covenants,
18 whether or not they are found to have breached any specific express contractual
19 term.

20 259. Plaintiffs and Class members are entitled to damages, including
21 compensatory damages and restitution, declaratory and injunctive relief, and
22 attorney fees, costs, and expenses.

23 **H. COUNT VIII – VIOLATIONS OF OKLAHOMA**
24 **CONSUMER PROTECTION ACT, OKLA. STAT., TIT. 15,**
CH. 20 §§ 751, *ET SEQ.*

25 260. Plaintiffs incorporate by reference all allegations of the preceding
26 paragraphs as though fully set forth herein.

27 261. Plaintiffs bring this Count against Defendants on behalf of the
28 Oklahoma Subclass.

1 262. Defendants are “persons,” as defined by Okla. Stat. tit. 15, § 752(1).

2 263. Defendants offer, sell, and distribute goods, services, and other things
3 of value which constitute “consumer transactions” as meant by Okla. Stat. tit. 15,
4 § 752(2).

5 264. Defendants, in the course of their business, engaged in unlawful
6 practices in violation of Okla. Stat. tit. 15, § 753, including the following:

- 7 a. Making false representations, knowingly or with reason to
8 know, as to the characteristics, uses, and benefits of the
9 subjects of their consumer transactions, in violation of Okla.
10 Stat. tit. 15, § 753(5);
- 11 b. Representing, knowingly or with reason to know, that the
12 subjects of their consumer transactions were of a particular
13 standard when they were of another, in violation of Okla. Stat.
14 tit 15, § 753(7);
- 15 c. Advertising, knowingly or with reason to know, the subjects of
16 their consumer transactions with intent not to sell as advertised,
17 in violation of Okla. Stat. tit 15, § 753(8);
- 18 d. Committing unfair trade practices that offend established
19 public policy and were immoral, unethical, oppressive,
20 unscrupulous, and substantially injurious to consumers as
21 defined by section 752(14), in violation of Okla. Stat. tit. 15, §
22 753(20); and
- 23 e. Committing deceptive trade practices that deceived or could
24 reasonably be expected to deceive or mislead a person to the
25 detriment of that person as defined by section 752(13), in
26 violation of Okla. Stat. tit. 15, § 753(20).

27 265. Defendants’ unlawful practices include:
28

- 1 a. Failing to implement and maintain reasonable security and
2 privacy measures to protect Plaintiffs' and Class members'
3 Personal and Medical Information, which was a direct and
4 proximate cause of the Data Breach;
- 5 b. Failing to identify foreseeable security and privacy risks,
6 remediate identified security and privacy risks, and adequately
7 improve security and privacy measures following previous data
8 incidents in the healthcare industry, which was a direct and
9 proximate cause of the Data Breach;
- 10 c. Failing to comply with common law and statutory duties
11 pertaining to the security and privacy of Plaintiffs' and Class
12 members' Personal and Medical Information, including duties
13 imposed by the FTC Act, HIPAA, and the CMIA;
- 14 d. Misrepresenting that they would protect the privacy and
15 confidentiality of Plaintiffs' and Class members' Personal and
16 Medical Information, including by implementing and
17 maintaining reasonable security measures;
- 18 e. Misrepresenting that they would comply with common law and
19 statutory duties pertaining to the security and privacy of
20 Plaintiffs' and Class members' Personal and Medical
21 Information, including duties imposed by the FTC Act, HIPAA,
22 and the CMIA;
- 23 f. Omitting, suppressing, and concealing the material fact that they
24 did not reasonably or adequately secure Plaintiffs' and Class
25 members' Personal and Medical Information; and
- 26 g. Omitting, suppressing, and concealing the material fact that they
27 did not comply with common law and statutory duties pertaining
28 to the security and privacy of Plaintiffs' and Class members'

1 Personal and Medical Information, including duties imposed by
2 the FTC Act and HIPAA.

3 266. Defendants' representations and omissions were material because
4 they were likely to deceive reasonable patient consumers about the adequacy of
5 Defendants' data security and ability to protect the confidentiality of their
6 Personal and Medical Information.

7 267. Defendants intended to mislead Plaintiffs and Class members and
8 induce them to rely on their misrepresentations and omissions.

9 268. Had Defendants disclosed to Plaintiffs and Class members that their
10 data security protocols and business emails (where highly sensitive personal data
11 was exchanged and/or stored) were not secure and, thus, vulnerable to attack,
12 Defendants would not have been able to continue in business and they would have
13 been forced to adopt reasonable data security measures and comply with the law.

14 269. The above unlawful practices and acts by Defendants were immoral,
15 unethical, oppressive, unscrupulous, and substantially injurious. These acts caused
16 substantial and continuous injury to Plaintiffs and Class members.

17 270. Defendants acted intentionally, knowingly, and maliciously to violate
18 Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiffs' and
19 the Class members' rights.

20 271. As a direct and proximate result of Defendants' unlawful practices,
21 Plaintiffs and Class members have suffered and will continue to suffer injury,
22 ascertainable losses of money or property, and monetary and non-monetary
23 damages, including time and expenses related to monitoring their credit and
24 medical accounts; an increased, imminent risk of fraud and identity theft; and loss
25 of value of their Personal and Medical Information.

26 272. Plaintiffs and Class members seek all monetary and non-monetary
27 relief allowed by law, including actual damages, civil penalties, and attorneys'
28 fees and costs.

1 **I. COUNT IX – VIOLATIONS OF CALIFORNIA UNFAIR**
2 **COMPETITION LAW, Cal. Bus. & Prof. Code §17200, et seq.**

3 273. Plaintiffs incorporate by reference all allegations of the preceding
4 paragraphs as though fully set forth herein.

5 274. Plaintiffs bring this Count against Defendants on behalf of the Class
6 or, alternatively, the California Subclass.

7 275. Defendants violated California’s Unfair Competition Law (“UCL”),
8 Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or
9 fraudulent business acts and practices and unfair, deceptive, untrue or misleading
10 advertising that constitute acts of “unfair competition” as defined in the UCL,
11 including, but not limited to, the following:

- 12 a. by representing and advertising that they would maintain
13 adequate data privacy and security practices and procedures to
14 safeguard their Personal and Medical Information from
15 unauthorized disclosure, release, data breach, and theft;
16 representing and advertising that they did and would comply
17 with the requirement of relevant federal and state laws pertaining
18 to the privacy and security of the Class’s Personal and Medical
19 Information; and omitting, suppressing, and concealing the
20 material fact of the inadequacy of the privacy and security
21 protections for the Class’ Personal and Medical Information;
- 22 b. by soliciting and collecting Class members’ Personal and
23 Medical Information with knowledge that the information would
24 not be adequately protected; and by storing Plaintiffs’ and Class
25 members’ Personal and Medical Information in an unsecure
26 electronic environment;
- 27 c. by failing to disclose the Data Breach in a timely and accurate
28 manner, in violation of Cal. Civ. Code §1798.82;

- 1 d. by violating the privacy and security requirements of HIPAA, 42
- 2 U.S.C. §1302d, *et seq.*;
- 3 e. by violating the CMIA, Cal. Civ. Code § 56, *et seq.*; and
- 4 f. by violating the CCRA, Cal. Civ. Code § 1798.82.

5 276. These unfair acts and practices were immoral, unethical, oppressive,
6 unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and
7 Class members. Defendants' practices were also contrary to legislatively declared
8 and public policies that seek to protect consumer data and ensure that entities that
9 solicit or are entrusted with personal data utilize appropriate security measures, as
10 reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et*
11 *seq.*, CMIA, Cal. Civ. Code § 56, *et seq.*, and the CCRA, Cal. Civ. Code §
12 1798.81.5.

13 277. As a direct and proximate result of Defendants' unfair and unlawful
14 practices and acts, Plaintiffs and the Class were injured and lost money or
15 property, including but not limited to the overpayments Defendants received to
16 take reasonable and adequate security measures (but did not), the loss of their
17 legally protected interest in the confidentiality and privacy of their Personal and
18 Medical Information, and additional losses described above.

19 278. Defendants knew or should have known that their computer systems
20 and data security practices were inadequate to safeguard Plaintiffs' and Class
21 members' Personal and Medical Information and that the risk of a data breach or
22 theft was highly likely. Defendants' actions in engaging in the above-named unfair
23 practices and deceptive acts were negligent, knowing and willful, and/or wanton
24 and reckless with respect to the rights of the Class.

25 279. Plaintiffs seek relief under the UCL, including restitution to the Class
26 of money or property that the Defendants may have acquired by means of
27 Defendants' deceptive, unlawful, and unfair business practices, declaratory relief,
28

1 attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and
2 injunctive or other equitable relief.

3 **J. COUNT X – VIOLATIONS OF CALIFORNIA CUSTOMER**
4 **RECORDS ACT, Cal. Civ. Code § 1798.80, et seq.**

5 280. Plaintiffs incorporate by reference all allegations of the preceding
6 paragraphs as though fully set forth herein.

7 281. Plaintiffs bring this Count against Defendants on behalf of the
8 California Subclass.

9 282. Section 1798.82 of the California Civil Code requires any “person or
10 business that conducts business in California, and that owns or licenses
11 computerized data that includes personal information” to “disclose any breach of
12 the security of the system following discovery or notification of the breach in the
13 security of the data to any resident of California whose unencrypted personal
14 information was, or is reasonably believed to have been, acquired by an
15 unauthorized person.” Under section 1798.82, the disclosure “shall be made in the
16 most expedient time possible and without unreasonable delay ...”

17 283. The CCRA further provides: “Any person or business that maintains
18 computerized data that includes personal information that the person or business
19 does not own shall notify the owner or licensee of the information of any breach
20 of the security of the data immediately following discovery, if the personal
21 information was, or is reasonably believed to have been, acquired by an
22 unauthorized person.” Cal. Civ. Code § 1798.82(b).

23 284. Any person or business that is required to issue a security breach
24 notification under the CCRA shall meet all of the following requirements:

- 25 a. The security breach notification shall be written in plain
26 language;
- 27 b. The security breach notification shall include, at a minimum, the
28 following information:

- i. The name and contact information of the reporting person or business subject to this section;
- ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
- iii. If the information is possible to determine at the time the notice is provided, then any of the following:
 1. The date of the breach;
 2. The estimated date of the breach; or
 3. The date range within which the breach occurred.The notification shall also include the date of the notice.
- iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;
- v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
- vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver’s license or California identification card number.

285. The Data Breach described herein constituted a “breach of the security system” of Defendants.

286. As alleged above, Defendants unreasonably delayed informing Plaintiffs and Class members about the Data Breach affecting their Personal and Medical Information, even after Defendants knew the Data Breach had occurred.

1 287. Defendants failed to disclose to Plaintiffs and the Class, without
2 unreasonable delay and in the most expedient time possible, the breach of security
3 of their unencrypted, or not properly and securely encrypted, Personal and
4 Medical Information when Defendants knew or reasonably believed such
5 information had been compromised.

6 288. Defendants’ ongoing business interests gave Defendants incentive to
7 conceal the Data Breach from the public to ensure continued revenue.

8 289. Upon information and belief, no law enforcement agency instructed
9 Defendants that timely notification to Plaintiffs and the Class would impede its
10 investigation.

11 290. As a result of Defendants’ violation of Cal. Civ. Code § 1798.82,
12 Plaintiffs and the Class were deprived of prompt notice of the Data Breach and
13 were thus prevented from taking appropriate protective measures, such as securing
14 identity theft protection or requesting a credit freeze. These measures could have
15 prevented some of the damages suffered by Plaintiffs and Class members because
16 their stolen information would have had less value to identity thieves.

17 291. As a result of Defendants’ violation of Cal. Civ. Code § 1798.82,
18 Plaintiffs and the Class suffered incrementally increased damages separate and
19 distinct from those simply caused by the Data Breach itself.

20 292. Plaintiffs and the Class seek all remedies available under Cal. Civ.
21 Code § 1798.84, including but not limited to, the damages suffered by Plaintiffs
22 and the other Class members as alleged above, and equitable relief.

23 293. Defendants’ misconduct as alleged herein is fraud under Cal. Civ.
24 Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to
25 the Defendants conducted with the intent on the part of Defendants of depriving
26 Plaintiffs and the Class of “legal rights or otherwise causing injury.” In addition,
27 Defendants’ misconduct as alleged herein is malice or oppression under Cal. Civ.
28 Code § 3294(c) in that it was despicable conduct carried on by Defendants with a

1 willful and conscious disregard of the rights or safety of Plaintiffs and the Class
2 and despicable conduct that has subjected Plaintiffs and the Class to cruel and
3 unjust hardship in conscious disregard of their rights. As a result, Plaintiffs and the
4 Class are entitled to punitive damages against Defendants under Cal. Civ. Code §
5 3294(a).

6 **K. COUNT XI – VIOLATIONS OF CALIFORNIA**
7 **CONFIDENTIALITY OF MEDICAL INFORMATION ACT,**
8 **Cal. Civ. Code § 56, *et seq.***

9 294. Plaintiffs incorporate by reference all allegations of the preceding
10 paragraphs as though fully set forth herein.

11 295. Plaintiffs bring this Count against Defendants on behalf of the Class
12 or, alternatively, the California Subclass.

13 296. Defendants are “provider[s] of healthcare,” as defined in Cal. Civ.
14 Code § 56.06, and are therefore subject to the requirements of the CMIA, Cal.
15 Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

16 297. Defendants are persons licensed under California under California’s
17 Business and Professions Code, Division 2. *See* Cal. Bus. Prof. Code § 4000, *et*
18 *seq.* Defendants therefore qualify as “provider[s] of healthcare,” under the CMIA.

19 298. Plaintiffs and the Class are “patients,” as defined in CMIA, Cal. Civ.
20 Code § 56.05(k) (“‘Patient’ means any natural person, whether or not still living,
21 who received healthcare services from a provider of healthcare and to whom
22 medical information pertains.”).

23 299. Defendants disclosed “medical information,” as defined in CMIA,
24 Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent,
25 in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to
26 unauthorized individuals in the Data Breach resulted from the affirmative actions
27 of Defendants’ employees, which allowed the hackers to see and obtain Plaintiffs’
28 and the Class members’ medical information.

1 300. Defendants’ negligence resulted in the release of individually
2 identifiable medical information pertaining to Plaintiffs and the Class to
3 unauthorized persons and the breach of the confidentiality of that information.
4 Defendants’ negligent failure to maintain, preserve, store, abandon, destroy,
5 and/or dispose of Plaintiffs’ and Class members’ medical information in a manner
6 that preserved the confidentiality of the information contained therein, in violation
7 of Cal. Civ. Code §§ 56.06 and 56.101(a).

8 301. Defendants’ computer and email systems and protocols did not
9 protect and preserve the integrity of electronic medical information in violation of
10 Cal. Civ. Code § 56.101(b)(1)(A).

11 302. Plaintiffs and the Class were injured and have suffered damages, as
12 described above, from Defendants’ illegal disclosure and negligent release of their
13 medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and
14 therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual
15 damages, nominal statutory damages of \$1,000, punitive damages of \$3,000,
16 injunctive relief, and attorney fees, expenses and costs.

17 **L. COUNT XII – VIOLATIONS OF WASHINGTON’S**
18 **UNIFORM HEALTH CARE INFORMATION ACT, WASH.**
19 **REV. CODE § 70.02.045, § 70.02.170**

20 303. Plaintiffs incorporate by reference all allegations of the preceding
21 paragraphs as though fully set forth herein.

22 304. Plaintiffs bring this Count against Defendants on behalf of the
23 Washington Subclass.

24 305. As a result of conducting their healthcare business and offering
25 medical services in Washington, Defendants possessed highly sensitive personal
26 and medical information, including healthcare information, belonging to the
27 members of the Washington Subclass.
28

1 306. Defendants released the Personal and Medical Information belonging
2 to members of the Washington Subclass without authorization, in violation of
3 Wash. Rev. Code § 70.02.045.

4 307. The members of the Washington Subclass were injured and have
5 suffered damages from Defendants’ illegal disclosure and negligent release of
6 their Personal and Medical Information, including healthcare information, in
7 violation of Wash. Rev. Code § 70.02.045.

8 308. The Washington Subclass seeks relief under Wash. Rev. Code §
9 70.02.170, including but not limited to actual damages, nominal damages,
10 injunctive relief, and/or attorney’s fees and costs.

11 **M. COUNT XIII – VIOLATIONS OF WASHINGTON’S**
12 **CONSUMER PROTECTION ACT, WASH. REV. CODE §**
13 **19.86.020, ET SEQ.**

14 309. Plaintiffs incorporate by reference all allegations of the preceding
15 paragraphs as though fully set forth herein.

16 310. Plaintiffs bring this Count against Defendants on behalf of the
17 Washington Subclass.

18 311. Defendants engaged in deceptive, unfair, and unlawful trade acts or
19 practices in the conduct of trade or commerce, in violation of Wash. Rev. Code §
20 19.86.020, including but not limited to the following:

- 21 a. Defendants misrepresented and fraudulently advertised material
22 facts to the Washington Subclass by representing and advertising
23 that they would maintain adequate data privacy and security
24 practices and procedures to safeguard Washington Class
25 Members’ Personal and Medical Information from unauthorized
26 disclosure, release, data breaches, and theft;
- 27 b. Defendants misrepresented material facts to the Washington
28 Subclass by representing and advertising that they did and would
comply with the requirements of relevant federal and state laws

1 pertaining to the privacy and security of Washington Subclass
2 members' Personal and Medical Information;

3 c. Defendants omitted, suppressed, and concealed the material fact
4 of the inadequacy of the privacy and security protections for
5 Washington Subclass members' Personal and Medical
6 Information;

7 d. Defendants engaged in deceptive, unfair, and unlawful trade acts
8 or practices by failing to maintain the privacy and security of
9 Washington Subclass members' Personal and Medical
10 Information, in violation of duties imposed by, and public
11 policies reflected in, applicable federal and state laws, resulting
12 in the Data Breach. These unfair acts and practices violated
13 duties imposed by laws that include the FTC Act, HIPAA, and
14 the state of Washington's regulations pertaining to Privacy of
15 Consumer Financial and Health Information (Wash. ADC 284-
16 04-300);

17 e. Defendants engaged in deceptive, unfair, and unlawful trade acts
18 or practices by failing to disclose the Data Breach to Washington
19 Subclass members in a timely and accurate manner, contrary to
20 the duties imposed by § 19.255.010(1); and

21 f. Defendants engaged in deceptive, unfair, and unlawful trade acts
22 or practices by failing to take proper action leading up to,
23 including, and following the Data Breach to enact adequate
24 privacy and security measures and protect Washington Subclass
25 members' Personal and Medical Information from further
26 unauthorized disclosure, release, data breaches, and theft.

1 312. As a direct and proximate result of Defendants’ deceptive trade
2 practices, Washington Subclass members suffered injury and damages as set forth
3 in this Complaint.

4 313. The above unfair and deceptive practices and acts by Defendants
5 were immoral, unethical, oppressive, and unscrupulous. These acts caused
6 substantial injury to consumers that these consumers could not reasonably avoid;
7 this substantial injury outweighed any benefits to consumers or to competition.

8 314. Defendants knew or should have known that their data security
9 practices were inadequate to safeguard Washington Subclass members’ Personal
10 and Medical Information and that the risk of a data breach was highly likely.
11 Defendants’ actions in engaging in the above-named unfair practices and
12 deceptive acts were negligent, knowing and willful, and/or wanton and reckless
13 with respect to the rights of members of the Washington Subclass.

14 315. Members of the Washington Subclass seek relief under Wash. Rev.
15 Code § 19.86.090, including but not limited to, actual damages, treble damages,
16 injunctive relief, and attorney’s fees and costs.

17 **N. COUNT XIV – VIOLATIONS OF TEXAS DECEPTIVE**
18 **TRADE PRACTICES ACT, TEX. BUS. & COMM. CODE §**
19 **17.41 ET SEQ.**

20 316. Plaintiffs incorporate by reference all allegations of the preceding
21 paragraphs as though fully set forth herein.

22 317. Plaintiffs bring this Count against Defendants on behalf of the Texas
23 Subclass.

24 318. In the course of their business, Defendants engaged in deceptive acts
25 and practices, misrepresentation, and the concealment, suppression, and omission
26 of material facts with respect to the sale and advertisement of their medical and
27 healthcare services, in violation of Tex. Bus. & Comm. Code § 17.41 *et seq.*,
28 including but not limited to the following:

- 1 a. Defendants misrepresented material facts by representing that
2 they would maintain adequate data privacy and security
3 practices and procedures to safeguard Texas Subclass members’
4 Personal and Medical Information from unauthorized disclosure,
5 release, data breaches, and theft, in violation of Tex. Bus. &
6 Comm. Code § 17.46 (5), (7), and (9).
- 7 b. Defendants misrepresented material facts to the Texas Subclass
8 by representing that they did and would comply with the
9 requirements of relevant federal and state laws pertaining to the
10 privacy and security of Texas Subclass members and Personal
11 and Medical Information, in violation of Tex. Bus. & Comm.
12 Code § 17.46 (5), (7), and (9);
- 13 c. Defendants omitted, suppressed, and concealed the material fact
14 of the inadequacy of the privacy and security protections for
15 Texas Subclass members’ Personal and Medical Information, in
16 violation of Tex. Bus. & Comm. Code § 17.46 (5), (7), and (9);
17 and
- 18 d. Defendants engaged in deceptive trade practices by failing to
19 maintain the privacy and security of Texas Subclass members’
20 Personal and Medical Information, in violation of duties
21 imposed by and public policies reflected in applicable federal
22 and state laws, resulting in the Data Breach.

23 319. The above unlawful and deceptive acts were immoral, unethical,
24 oppressive, and unscrupulous. These acts caused substantial injury to consumers
25 that the consumers could not reasonably avoid; this substantial injury outweighed
26 any benefits to consumers or to competition.

27 320. Defendants knew or should have known that their data security
28 practices were inadequate to safeguard Texas Subclass members’ Personal and

1 Medical Information and that risk of a data breach or theft of patients' highly
2 sensitive personal and medical information was highly likely. Defendants' actions
3 in engaging in the above-named unfair practices and deceptive acts were
4 negligent, knowing and willful, and/or wanton and reckless with respect to the
5 rights of members of the Texas Subclass.

6 321. As a direct and proximate result of Defendants' deceptive practices,
7 Texas Subclass members suffered injury and/or damages.

8 322. Texas Subclass members seek relief under Tex. Bus. & Comm. Code
9 § 17.50, including, but not limited to, injunctive relief, other equitable relief,
10 damages, and attorney's fees and costs.

11 **O. COUNT XV – DECLARATORY RELIEF**

12 323. Plaintiffs incorporate by reference all allegations of the preceding
13 paragraphs as though fully set forth herein.

14 324. Plaintiffs bring this Count under the federal Declaratory Judgment
15 Act, 28 U.S.C. §2201.

16 325. As previously alleged, Plaintiffs and members of the Class entered
17 into an implied contract that required Defendants to provide adequate security for
18 the Personal and Medical Information it collected from Plaintiffs and the Class.

19 326. Defendants owe a duty of care to Plaintiffs and the members of the
20 Class that requires them to adequately secure Personal and Medical Information.

21 327. Defendants still possess Personal and Medical Information regarding
22 Plaintiffs and members of the Class.

23 328. Since the Data Breach, Defendants have announced few if any
24 changes to their data security infrastructure, processes or procedures to fix the
25 vulnerabilities in their computer and email systems and/or security practices which
26 permitted the Data Breach to occur and go undetected for months and, thereby,
27 prevent further attacks.

28

1 329. Defendants have not satisfied their contractual obligations and legal
2 duties to Plaintiffs and the Class. In fact, now that Defendants’ insufficient data
3 security is known to hackers, the Personal and Medical Information in
4 Defendants’ possession is even more vulnerable to cyberattack.

5 330. Actual harm has arisen in the wake of the Data Breach regarding
6 Defendants’ contractual obligations and duties of care to provide security
7 measures to Plaintiffs and the members of the Class. Further, Plaintiffs and the
8 members of the Class are at risk of additional or further harm due to the exposure
9 of their Personal and Medical Information and Defendants’ failure to address the
10 security failings that lead to such exposure.

11 331. There is no reason to believe that Defendants’ security measures are
12 any more adequate now than they were before the breach to meet Defendants’
13 contractual obligations and legal duties.

14 332. Plaintiffs, therefore, seek a declaration that Defendants’ existing
15 security measures do not comply with their contractual obligations and duties of
16 care to provide adequate security and that to comply with their contractual
17 obligations and duties of care, Defendants must implement and maintain
18 additional security measures.

19 **VII. PRAYER FOR RELIEF**

20 WHEREFORE, Plaintiffs and the Class pray for judgment against
21 Defendants as follows:

- 22 a. An order certifying this action as a class action under Fed. R.
23 Civ. P. 23, defining the Class as requested herein, appointing
24 the undersigned as Class counsel, and finding that Plaintiffs are
25 proper representatives of the Class requested herein;
- 26 b. A judgment in favor of Plaintiffs and the Class awarding them
27 appropriate monetary relief, including actual and statutory
28 damages (including statutory damages under the CMIA),

1 punitive damages, attorney fees, expenses, costs, and such
2 other and further relief as is just and proper.

3 c. An order providing injunctive and other equitable relief as
4 necessary to protect the interests of the Class and the general
5 public as requested herein, including, but not limited to:

- 6 i. Ordering that Defendants engage third-party security
7 auditors/penetration testers as well as internal security
8 personnel to conduct testing, including simulated
9 attacks, penetration tests, and audits on Defendants'
10 systems on a periodic basis, and ordering Defendants to
11 promptly correct any problems or issues detected by
12 such third-party security auditors;
- 13 ii. Ordering that Defendants engage third-party security
14 auditors and internal personnel to run automated security
15 monitoring;
- 16 iii. Ordering that Defendants audit, test, and train their
17 security personnel regarding any new or modified
18 procedures;
- 19 iv. Ordering that Defendants segment customer data by,
20 among other things, creating firewalls and access
21 controls so that if one area of Defendants' systems is
22 compromised, hackers cannot gain access to other
23 portions of Defendants' systems;
- 24 v. Ordering that Defendants cease transmitting Personal
25 and Medical Information via unencrypted email;
- 26 vi. Ordering that Defendants cease storing Personal and
27 Medical Information in email accounts;
- 28

- vii. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services;
 - viii. Ordering that Defendants conduct regular database scanning and securing checks;
 - ix. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
 - x. Ordering Defendants to meaningfully educate their current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves;
- d. An order requiring Defendants to pay the costs involved in notifying the Class members about the judgment and administering the claims process;
 - e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
 - f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

1 DATED: January 27, 2021

GREEN & NOBLIN, P.C.

2
3
4 By: /s/ Robert S. Green
Robert S. Green

5 James Robert Noblin
6 Emrah M. Sumer
7 2200 Larkspur Landing Circle, Suite 101
8 Larkspur, CA 94939
9 Telephone: (415) 477-6700
Facsimile: (415) 477-6710

10 William B. Federman*
11 wbf@federmanlaw.com
12 Oklahoma Bar No. 2853
13 **FEDERMAN & SHERWOOD**
14 10205 N. Pennsylvania Ave.
15 Oklahoma City, OK 73120
16 Telephone: (405) 235-1560
17 Facsimile: (405) 239-2112

18 *Pro Hac Vice application to be submitted

19 *Counsel for Plaintiffs and the Proposed*
20 *Class*

EXHIBIT 1



December 16, 2020

To Parent or Legal Guardian of
Carter Bean
1404 Concord Ln.
Edmond, OK 73003-6131

P21T1275



Notice of Data Security Event

To Parent or Legal Guardian of Carter Bean:

We are writing to inform you of a data security event that occurred at MEDNAX Services, Inc. ("MEDNAX") and may have impacted your child's personal information. MEDNAX provides revenue cycle management and other administrative services to its affiliated physician practice groups, including Pediatrix Medical Group of Oklahoma, P.C., from which your child may have received services.

What happened?

On June 19, 2020, MEDNAX discovered that an unauthorized third party gained access to certain Microsoft Office 365-hosted MEDNAX business email accounts through phishing. "Phishing" occurs when an email is sent that looks like it is from a trustworthy source, but it is not. The phishing email prompts the recipient to share or give access to certain information. Upon discovery of this event, MEDNAX immediately took action to prevent any further unauthorized activity, began an investigation, and engaged a national forensic firm.

Based on the investigation, the unauthorized party was able to access certain business email accounts between June 17, 2020 and June 22, 2020. The event was limited to a small number of business email accounts. Those email accounts are separate from MEDNAX's internal network and systems, which were not involved in the event. Even though a thorough investigation was conducted, it was not possible to conclusively determine whether personal information was actually accessed by the unauthorized party. Based on the data analysis that was performed and ultimately completed in late November 2020, we were able to determine which individuals may have had personal information in the impacted business email accounts. Based upon our thorough review of this matter, we are not aware of any actual or attempted misuse of personal information as a result of this event. However, we are notifying you because your child's personal information may have been in one or more of the impacted business email accounts.

What information may have been involved?

The patient information may have included: (1) patient contact information (such as patient name, guarantor name, address, email address, and date of birth); (2) health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number); (3) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (4) billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by your child's provider). Please note that not all data fields may have been involved for all individuals.

What we are doing.

MEDNAX takes the security of personal information seriously. As soon as we discovered the phishing event, we immediately took action to prevent any further unauthorized activity, including resetting user passwords for business

email accounts where unauthorized activity was detected. We have and continue to enhance our security controls as appropriate to minimize the risk of any similar event in the future.

What you can do.

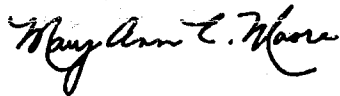
The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your child's personal information. We encourage you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all account activity is valid; any questionable charges should be promptly reported to the provider's billing office, or for insurance statements, to your insurance company.

For more information

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit www.emailevent.kroll.com, or call toll-free 1-833-971-3267. This call center is open from 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding major U.S. holidays.

We regret that this event occurred and are very sorry for any distress or inconvenience this event may cause you.

Sincerely,



Mary Ann E. Moore
Chief Compliance Officer

Reference Guide**Review Your Account Statements**

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	888-298-0045	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Mednax, Pediatrix Hit with Class Action Over June 2020 Data Breach Affecting Nearly 1.3M Patients](#)
