THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF TEXAS

JAMES LOGAN and NATHAN BAXTER, individually and on behalf of all others similarly situated, Plaintiffs, v. MARKER GROUP, INC., a Texas corporation, Defendant.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs James Logan and Nathan Baxter ("Plaintiffs") brings this Class Action Complaint against Marker Group, Inc. ("Marker Group" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard medical records and other documentation containing sensitive information that Plaintiffs and Class Members in mass tort litigations against Defendant's customers entrusted to it. These medical records and other documentation, such as plaintiff fact sheets, contain sensitive information, including, without limitation, names, Social Security numbers, dates of birth, patient numbers, and/or addresses (collectively, "personally identifiable information" or "PII") as well as medical treatment and diagnosis information and/or personal health information (collectively, "protected health information" or "PHI").[1] Plaintiffs allege that Defendant failed to comply with

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an

industry standards to protect information systems that contain that PII and PHI, and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other Class Members that their PII and PHI had been accessed and potentially acquired by an unauthorized third-party. Plaintiffs seek, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised, to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future, to destroy information no longer necessary to retain for purposes for which the information was first obtained from Class Members, and to provide a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protective services for their respective lifetimes as Plaintiffs and Class Members will be at an increased risk of identity theft due to the conduct of Marker Group as described herein.

2. According to its website, Marker Group provides "record collection, medical review, data analysis, and many other litigation support services" to some of "the world's most prestigious defense law firms."[2] For its customers, Marker Group offers services to retrieve, collect, and store medical records and other documentation in large scale. Marker Group offers these services in large multi-district litigations ("MDL") involving thousands of individuals who have brought personal injury claims against Marker Group's clients. In relation to these services, Defendant operates an ftp platform system that allows medical records and other personal information and documentation to be uploaded, stored, sorted, and analyzed.

3. In the ordinary course of litigating against Defendant's corporate customers, individuals such as Plaintiffs are regularly required to provide their PII and PHI to Marker Group

individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[2] https://www.marker-group.com/ (last visited Jan. 11, 2022).

directly by uploading it to Marker Group's litigation portal.

4. For their cases proceeding in *In Re. Proton-Pump Inhibitor ("PPI") Products Liability Litigation* ("MDL-2789") pending in the United States District Court, District of New Jersey, Plaintiffs James Logan and Nathan Baxter, and other Class Members, were required to upload their plaintiff fact sheets, medical, pharmacy, and insurance records, and executed authorizations for obtaining medical records, employment, and insurance documents to the global ShareFile site maintained by Marker Group. Pursuant to Case Management Order No. 9 in that litigation, uploading required documents to the ShareFile site maintained by Marker Group is the method to effectuate service of said documents on the Marker Group in that MDL.[3]

5. Marker Group promotes that it is the "first ISO 27001:2013 certified national record collection and medical review vendor, employing the highest standards in the world to protect your data." [4]

6. Defendant states that it maintains data on "Marker-owned servers" and not cloud-based servers "to ensure the maximum level of control and security."[5]

7. Defendant's website states that "Marker Group has set standards and invented new best practices for digital security and access in the litigation support industry. Our philosophy is to protect client data at least as securely as we would want our personal data protected."[6]

8. On September 3, 2021, Defendant noticed "suspicious activity" on its computer network and later determined that files were accessed by an "unknown, unauthorized third-party" (the "Data Breach").[7]

---

[3] https://www.njd.uscourts.gov/sites/njd/files/CaseManagementOrderNo9_0.pdf (last visited Jan. 11, 2022).
[4] https://www.marker-group.com/ (last visited Jan. 11, 2022).
[5] https://www.marker-group.com/security-technology/security/ (last visited Jan. 11, 2022).
[6] https://www.marker-group.com/security-technology/ (last visited Jan. 11, 2022).
[7] https://ago.vermont.gov/blog/2021/12/23/the-marker-group-data-breach-notice-to-consumers/?utm_source=rss&utm_medium=rss&utm_campaign=the-marker-group-data-breach-notice-to-consumers (last visited Jan. 11, 2022).

9. In its Notice of Data Breach dated December 23, 2021, Marker Group advises that the files accessed contained PII and PHI.[8] However, the Notice provides scant other information, including how long these unauthorized third-parties had access to the medical records and other sensitive information of Plaintiffs and Class Members.

10. Further, Marker Group has failed to explain why it took more than two months to begin notifying individuals that their PHI and PII had been accessed by an unauthorized third-party.

11. This case involves a breach of a computer system by an unknown third-party, resulting in the unauthorized disclosure and potential acquisition of the PII and PHI of Plaintiffs and Class Members to unknown third-parties. As a result of Defendant's failure to implement and follow basic security procedures, the PII and PHI of Plaintiffs and Class Members was accessed and/or acquired and is now in the hands of criminals. Plaintiffs and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Marker Group's failures.

12. Additionally, as a result of Defendant's failure to follow federally-prescribed, industry standard security procedures, Plaintiffs and Class Members received only a diminished value of the services Defendant was to provide.

13. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access, intrusion, and/or acquisition.

14. Defendant admits that the unencrypted PII and PHI exposed to unauthorized access

[8] *Id.*

included names, Social Security numbers, dates of birth, and various types of medical records containing medical treatment, diagnosis, and insurance information.[9]

15. The exposed PII and PHI of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and/or specific, sensitive medical information.

16. The Data Breach occurred due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiffs and Class Members. Defendant waited months to report the Data Breach to Plaintiffs and Class Members and still maintains as secret the specific vulnerabilities and root causes of the Data Breach. Plaintiffs and Class Members also remain unaware of precisely what information was accessed and for how long.

17. Plaintiffs bring this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to adequately protect the PII and PHI of Plaintiffs and Class Members and failure to warn Plaintiffs and Class Members of Defendant's inadequate information security practices. Defendant's conduct amounts to negligence and violates federal and state statutes.

18. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and,

[9] https://www.prnewswire.com/news-releases/the-marker-group-provides-notice-of-data-privacy-incident-301452043.html (last visited Jan. 11, 2022).

significantly (iv) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third-parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

19. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

20. Plaintiff James Logan is a citizen and resident of Georgia.

21. Plaintiff Nathan Baxter is a citizen and resident of California.

22. Defendant The Marker Group, Inc. is a for-profit corporation incorporated in the state of Texas and headquartered in Houston.

23. Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

24. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity, as both Plaintiff James Logan and Plaintiff Nathan Baxter are citizens of states different from Marker Group.

25. This Court has personal jurisdiction over Defendant named in this action because Defendant is headquartered in Houston, Texas and conducts substantial business in this District.

26. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to

Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

I. Background

27. Defendant is a company that provides medical records collection, medical review, data analysis and other litigation support services for large defense firms. According to Defendant's website, Marker Group is considered "an innovative and cost-effective leader in defense litigation management and support."[10]

28. Marker Group provides an online platform which serves as a centralized location for parties in large litigation matters to manage medical records, plaintiff fact sheets, and other discovery materials.[11]

29. Depending upon the litigation and the functions specified by Defendant's customers, parties in a large litigation matter, such as a mass tort MDL, can upload medical records and litigation documents to Marker Group's portal where it is housed for continued access by the parties.

30. Due to the nature of the services provided, Defendant routinely acquires and stores PII and PHI of plaintiffs in litigation matters.

31. Plaintiffs and Class Members are plaintiffs in MDL matters in which the defendant in that litigation has contracted to use Marker Group. Plaintiffs and Class Members were required to upload their medical, pharmacy, and insurance records and other sensitive and confidential information onto the Marker Group portal as a condition of their participation in the MDL litigation.

32. Plaintiffs and Class Members entrusted this sensitive and confidential information

[10] https://www.marker-group.com/our-services/ (last visited January 12, 2022).
[11] https://www.marker-group.com/our-services/fact-sheet-services-statistics/ (last visited January 12, 2022).

to Defendant to store and manage. This sensitive and confidential information included, without limitation, their names, Social Security numbers, dates of birth, and addresses, as well as medical treatment and diagnosis information and other personal health information, many of which are static, do not change, and can be used to commit myriad financial crimes.

33. The PHI stored on Marker Group's servers is sensitive and confidential, and is protected, private medical information. This includes medical treatment information and other PHI that may divulge underlying mental or physical diagnoses, as well as prescription, testing/laboratory results, physician's notes, and other personal health information.

34. Defendant has not yet made Plaintiffs and Class Members aware of the extent to which the above referenced records and documentation were accessed and/or acquired or when the Marker Group's data systems were compromised.

35. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII and PHI.

36. Defendant had a duty to adopt reasonable measures to protect the PII and PHI of Plaintiffs and Class Members from unauthorized disclosure to third-parties.

II. The Data Breach

37. Defendant admitted in the Notice of Data Breach that an unknown, unauthorized third-party accessed Defendant's server associated with its litigation portal. Defendant also admitted that an unauthorized third-party accessed files containing sensitive information, including names, Social Security numbers, dates of birth, addresses and medical records.

38. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the adequacy of any remedial measures undertaken to ensure a breach does not

occur again have not been transparently shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

39. The PII and PHI of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs and Class Members.

40. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained and stored belonging Plaintiffs and Class Members, causing the exposure of this PII and PHI.

III. The Health Care Sector is Particularly Susceptible to Data Breaches

41. Defendant was on notice that companies with health care information are routine targets for data breaches.

42. Defendant was also on notice that the FBI has been concerned about data security of health care information. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the health care industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting health care related systems, perhaps for the purpose of obtaining the Protected Health care Information (PHI) and/or Personally Identifiable Information (PII)."[12]

43. The American Medical Association ("AMA") has also warned health care companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[13]

[12] Jim Finkle, *FBI Warns Health care Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-health care-fbi/fbi-warns-health care-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Jan. 11, 2022).

[13] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019),

44. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[14] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[15] That trend continues.

45. The health care sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[16] Indeed, when compromised, health care related data is among the most sensitive and personally consequential. A report focusing on health care breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[17] Almost 50 percent of the victims lost their health care coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[18]

46. Health care related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security

---

available at: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Jan. 11, 2022).

[14] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/post/data-breaches-up-nearly-45-percent-according-to-annual-review-by-identity-theft-resource-center-and-cyberscout/(last visited Jan. 11, 2022).

[15] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last visited Sept. 18, 2020).

[16] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited Sept. 18, 2020).

[17] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Sept. 28, 2020).

[18] *Id.*

incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[19] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[20]

IV. Defendant Acquires, Collects, and Stores the PII and PHI of Plaintiffs and Class Members.

47. Marker Group acquired, collected, and stored the PII and PHI of Plaintiffs and Class Members.

48. By obtaining, collecting, and storing the PII and PHI of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

49. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and implicitly relied on Defendant to keep their PII and PHI confidentialand securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

V. Securing PII and PHI and Preventing Breaches

50. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII and PHI of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially outdated information.

---

[19] *2019 HIMSS Cybersecurity Survey*, *available at*: https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Jan. 13, 2022).

[20] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Jan. 13, 2022).

51. Defendant's negligence in safeguarding the PII and PHI of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

52. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiffs and Class Members from being compromised.

53. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[21] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,employer or taxpayer identification number."[22]

54. The ramifications of Defendant's failure to keep secure the PII and PHI of Plaintiffs and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

VI. Value of Personal Identifiable Information

55. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[23] Experian reports that a stolen credit or

[21] 17 C.F.R. § 248.201 (2013).
[22] *Id.*
[23] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct.16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web- how-much-it-costs/ (last visited Jan. 13, 2022).

debit card number can sell for $5 to $110 on the dark web.[24]

56. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety offraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

57. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good creditto apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment foritems you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[25]

58. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number withoutsignificant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

59. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited

[24] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask- experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark- web/ (last visited Jan. 13, 2022).

[25] *Identity Theft and Your Social Security Number*, Social Security Administration, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 13, 2022).

into the new Social Security number."[26]

60. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, medical records, and potentially date of birth.

61. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[27]

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

63. The PII and PHI of Plaintiffs and Class Members was taken by hackers to engage in identity theft and/or to sell to other criminals who will purchase the PII and PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

64. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting

[26] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 13, 2022).

[27] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 13, 2022).

from data breaches cannot necessarily rule out all future harm.[28]

65. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs and Class Members, including Social Security numbers and medical records, and of the foreseeable consequences that wouldoccur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

67. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's file servers, amounting to potentially tens or hundreds of thousands of individuals' detailed, personal information and thus, the significant number of individuals who would be harmed by the exposure ofthe unencrypted data.

68. To date, Defendant has offered Plaintiffs and Class Members only two years of identity protection services through Experian Creditworks™ 3B. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII and PHI at issue here.

69. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiffs and Class Members.

VII. Marker Group's Conduct Violates HIPAA

70. Title II of HIPAA contains what are known as the Administrative Simplification

[28] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 13, 2022).

provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

71. Defendant is aware of the existence of HIPAA's Security Standards, and expressly refers to HIPAA's Security Standards on its website.[29]

72. Defendant's Data Breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs' and Class Members' PII and PHI.

73. In addition, Defendant's Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PII and/or PHI when it was no longer necessary and/or had honored its customer's obligations to Plaintiffs and Class Members.

74. Defendant's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Marker Group creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information

[29] https://www.marker-group.com/security-technology/security/

systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*; and

k. Retaining information past a recognized purpose and not deleting it.

75. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay

and ***in no case later than 60 days following discovery of the breach***."[30]

76. While monetary relief may cure some of Plaintiffs' and Class Members' injuries, because Defendant has failed to comply with industry standards, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the protected health information and other PII of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs' and Class Members' protected health information and other PII remains at risk of subsequent Data Breaches.

VIII. Marker Group Failed to Comply with FTC Guidelines

77. Marker Group was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

78. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

79. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[32] The guidelines note that businesses should protect the personal customer information that they keep; properly

[30] Breach Notification Rule, U.S. Dep't of Health & Human Services, *available at*: hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Jan. 11, 2022).
[31] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 13, 2022).
[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 13, 2022).

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

80. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[33]

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

82. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

83. Defendant was at all times fully aware of its obligation to protect Plaintiffs's and Class Members' PII and PHI because of its position as a software vendor for health care organizations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[33] FTC, *Start With Security*, *supra*.

IX. Plaintiffs' Experiences

84. Plaintiffs James Logan and Nathan Baxter have cases pending in the PPI MDL for which Marker Group has been contracted by the defendants in that action for the transmittal and storage of medical records, plaintiff fact sheets, and other documentation related to the litigation.

85. At the time of the Data Breach, Defendant retained the name, Social Security number, and medical records of Plaintiffs, as well as thousands of other individuals in its data system.

86. Plaintiff James Logan received Defendant's Notice of Data Breach on or around January 14, 2022. The notice stated that Plaintiff's name, Social Security number, date of birth, medical records containing treatment and insurance information were contained in files accessed and potentially acquired during the Data Breach.

87. As a result of receiving the Notice of Data Breach, Plaintiff Logan spent time dealing withthe consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

88. Shortly before receiving the Notice of Data Breach, Plaintiff Logan had encountered a situation with his treating physician in which it appeared that information unrelated to him had been transmitted to his physician under his name. Plaintiff Logan now realizes that this erroneous information may have been transmitted as a result of the Data Breach.

89. Additionally, Plaintiff James Logan is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

90. Plaintiff James Logan stores any documents containing his sensitive PII or PHI in a

safe and secure location.

91. Since the Data Breach, Plaintiff Nathan Baxter has received a barrage of calls regarding Medicare insurance coverage. Because the callers relay information and offers that contradict his current coverage (such as offers to decrease his premium when he has none), Plaintiff Nathan Baxter has realized that these calls are not legitimate.

92. Plaintiff Baxter has also recently started receiving unsolicited loan offers which contain his personal information.

93. Plaintiff Baxter is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

94. Plaintiff Baxter stores any documents containing his sensitive PII or PHI in a safe and secure location.

95. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII and PHI —a form of intangible property that Plaintiffs entrusted Defendant, which was compromised in and as a result of the Data Breach.

96. Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have increased concerns for the loss of their privacy.

97. Plaintiffs have suffered injury arising from the present and continuing risk of fraud, identity theft, and misuse resulting from their PII and PHI, especially their Social Security number, in combination with their names, being placed in the hands of unauthorized third parties and possibly criminals.

98. Plaintiffs have a continuing interest in ensuring that their PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

99. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

100. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All United States residents whose PII and/or PHI was actually or potentially compromised in the Data Breach first reported by Marker Group, Inc. in December 2021 (the "Nationwide Class" or "Class").

101. Plaintiff Nathan Baxter also brings claims under California law on behalf of himself and a California subclass defined as follows:

> All California residents whose PII and/or PHI was actually or potentially compromised in the Data Breach first reported by Marker Group, Inc. in December 2021 (the "California Subclass").

102. Collectively the Nationwide Class and California Subclass shall be collectively referred to as the "Class."

103. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff members.

104. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

105. Numerosity, Fed R. Civ. P. 23(a)(1): The members of the Class are so numerous that joinder of all members is impracticable. Based upon the number of filed cases in the PPI MDL,

Plaintiffs is informed and believes that the Data Breach affected more than 14,000 individuals. The Class is identifiable within Defendant's records.

106. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII and PHI of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

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

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

107. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendant's misfeasance. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

108. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

109. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

110. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fairand efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

111. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costsof individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that

experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicativeof this litigation.

112. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

113. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

114. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

115. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, andsafeguarding their PII and PHI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Plaintiffs and Class Members are third-party beneficiaries of contracts between Defendant and law firms which contracted for Marker Group to provide services collecting PII and PHI from individual plaintiffs in litigation matters, including Plaintiffs and Class Members;

g. Whether Defendant breached these contracts of which Plaintiffs and Class Members are third-party beneficiaries;

h. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

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

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members; and,

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

117. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

118. As a condition of litigating against Defendant's clients, Plaintiffs and Class Members were obligated to provide Marker Group their PII and PHI.

119. Marker Group owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, using, and protecting their PII and PHI from unauthorized third parties.

120. Plaintiffs and Class Members entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for litigation purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

121. Marker Group had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and Class Members could and would suffer if the PII and PHI were wrongfully disclosed.

122. Defendant also knew of the serious harms and the types of harm that Plaintiffs and the Class Members could and would suffer if the PII and PHI were wrongfully disclosed, that disclosure was not fixed, or Plaintiffs and the Class were not told about the disclosure in a timely manner.

123. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiffs and Class Members in Defendant's possession was adequately secured and protected.

124. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiffs and Class Members.

125. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential PII and PHI, a necessary and required part of participating in litigation involving from Defendant's customers and/or using Defendant's services.

126. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class or between Defendant and its customers.

127. Defendant had a common law duty to prevent foreseeable harm to those whose PII and PHI it stored. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices.

128. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

129. Plaintiffs and Nationwide Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and Class Members, the critical importance of providing adequate security ofthat PII, and the necessity for encrypting PII stored on Defendant's systems. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Marker Group knew or should have known that it was more likely than not Plaintiffs and Class Members would be harmed.

130. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class

Members.

131. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiffs and Class Members, including basic encryption techniques freely available to Defendant.

132. Plaintiffs and Class Members had no ability to protect their PII and PHI that were and remain in Defendant's possession.

133. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

134. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

135. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

136. Defendant has admitted that the PII and PHI of Plaintiffs and Class Members was wrongfully disclosed and/or lost to unauthorized third persons as a result of the Data Breach.

137. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and Class Members during the time the PII and PHI was within Defendant's possession or control.

138. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiffs

and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

139. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiffs and Class Members in the face of increased risk of theft.

140. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII and PHI Plaintiffs and Class Members.

141. Defendant's failure to comply with industry and federal regulations further demonstrates Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting the PII and PHI of Plaintiffs and Class Members.

142. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

143. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII and PHI of Plaintiffs and Class Members would not have been compromised.

144. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The PII and PHI of Plaintiffs and Class Members was accessed and/or lost as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

145. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting

commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

147. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

148. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

149. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

150. Defendant's violations of HIPAA also constitute negligence *per se*.

151. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of health care information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to health care providers and the organizations they work for, but to any entity that may have access to health care information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

152. Plaintiffs and Class Members are within the class of persons that HIPAA privacy

laws were intended to protect.

153. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

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

155. As a direct and proximate result of Defendant's negligence and negligence *per se* Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

156. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks

of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

157. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

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

158. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98 as though fully set forth herein.

159. Plaintiffs and Class Members were required to provide their PII and PHI, including their names, Social Security numbers, addresses, dates of birth, telephone numbers, email addresses, and various health related information to Defendant as a condition of their use of Defendant's services. By providing their PII and PHI, and upon Defendant's acceptance of such information, Plaintiffs and all Class Members, on one hand, and Marker Group on the other hand, entered into implied-in-fact contracts for the provision of data security.

160. These implied-in-fact contracts obligated Marker Group to take reasonable steps to secure and safeguard the PII and PHI of Plaintiffs and Class Members, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen. The terms of these implied contracts are further described in the federal laws, state laws, and industry standards alleged above, and Defendant expressly assented to these terms in their public statements regarding data security described above.

161. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

162. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data and cyber security practices and policies were reasonable and consistent with industry standards.

163. Plaintiffs and Class Members would not have provided and entrusted their PII and PHI to Defendant in the absence of the implied contract or implied terms between them and Defendant. The safeguarding of the PII and PHI of Plaintiffs and Class Members was critical to realize the intent of the parties.

164. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their personal information and by failing to provide timely and accurate notice to them that PII and PHI was compromised as a result of the Data Breach.

165. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm

166. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

167. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

168. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

169. Defendant owed a duty to those individuals whose PII and PHI Defendant collected and stored as part of its services rendered, including that of Plaintiffs and Class Members, to keep their PII and PHI obtained as a condition thereof, confidential.

170. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiffs and Class Members.

171. Defendant allowed unauthorized and unknown third-parties access to and examination of the PII and PHI of Plaintiffs and Class Members, by way of Defendant's failure to protect its data systems.

172. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHI of Plaintiffs and Class Members is highly offensive to a reasonable person.

173. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII and PHI to Defendant as part of their litigation with Defendant's customers, but did so privately with an intention that the PII and PHI would be kept confidential andwould be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

174. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

175. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it acted with actual knowledge that its information security practices were inadequate and insufficient.

176. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

177. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiffs and Class Members was disclosed to third-parties without authorization, causing Plaintiffs and Class Members to suffer damages.

178. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

179. As a direct and proximate result of Defendant's invasion of privacy, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

180. Plaintiffs re-allege and incorporate by reference herein all of the allegations

contained in paragraphs 1 through 98.

181. Defendant benefited financially from receiving the PII and PHI of Plaintiffs and Class Members through its contracts with its customers for litigation support services. Defendant understood this benefit.

182. Defendant understood and appreciated that the PII and PHI of Plaintiffs and Class Members was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII and PHI.

183. Defendant also understood and appreciated that without the PII and PHI of Plaintiffs and Class Members, Defendant would not be able to perform the services it contracted for and for which it was paid by its customers.

184. Marker Group appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members.

185. The monies that Defendant received for these litigation support services were to be used by Marker Group, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures in order to secure the PII and PHI of Plaintiffs and Class Members, upon which Defendant relied.

186. But for Defendant's commitment to maintain privacy and confidentiality, the PII and PHI of Plaintiffs and Class Members would not have been transferred to and untrusted with Defendant. Indeed, if Marker Group had informed Plaintiffs and Class Members that their data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by the courts, its customers, or consumers.

187. As a result of Defendant's wrongful conduct, Marker Group have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members. Marker Group continue to benefit and profit from their retention and use of the PII and PHI of

Plaintiffs and Class Members while its value to Plaintiffs and Class Members has been diminished.

188. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining the PII and PHI of Plaintiffs and Class Members, while at the same time failing to maintain that information is secure from intrusion and theft by hackers and identity thieves.

189. Under principals of equity and good conscience, Defendant should not be permitted to retain the money it made from the use of the PII and PHI of Plaintiffs and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

190. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable benefits and proceeds they received as a result of the conduct alleged herein.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class)

191. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98 as though fully set forth herein.

192. At all times during Plaintiffs' and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of the PII and PHI that Plaintiffs and Class Members provided to Defendant.

193. As alleged herein and above, Defendant's relationships with Plaintiffs and Class Members were governed by terms and expectations that the PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third-parties.

194. Plaintiffs and Class Members provided PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third-parties.

195. Plaintiffs and Class Members also provided their PII and PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

196. Defendant voluntarily received in confidence the PII and PHI of Plaintiffs and Class Members with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third-parties.

197. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII and PHI of Plaintiffs and Class Members was disclosed and misappropriated to unauthorized third-parties beyond the confidence of Plaintiffs and Class Members, and without their express permission.

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

199. But for Defendant's disclosure in violation of the parties' understanding of confidence, the PII and PHI of Plaintiffs and Class Members would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of the PII and PHI of Plaintiffs and Class Members as well as the resulting damages.

200. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of the PII and PHI of Plaintiffs and Class Members. Defendant knew or should have known its methods of accepting and the PII and PHI of Plaintiffs and Class Members was inadequate as it relates to, at the very least, securing servers,

portals, and other data systems containing PII and PHI.

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

202. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members are entitled to recover actual, consequential, andnominal damages.

COUNT VI
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

203. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

204. Defendant owes duties of care to Plaintiffs and Class Members which requires Defendant to adequately secure their PII and PHI.

205. Defendant still possesses the PII and PHI of Plaintiffs and Class Members.

206. Defendant does not specify in its Notice of Data Breach letter what steps they have taken to prevent this from occurring again.

207. Plaintiffs and Class Members are at risk of harm due to the exposure of their PII and PHI and Defendant's failure to address the security failings that lead to such exposure.

208. Plaintiffs, therefore, seek a declaration that (1) each of Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect the PII and PHI of Plaintiffs and Class Members, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting 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;

g. Purchasing credit monitoring and identity theft restoration services for Plaintiffs and Class Members for a period of ten years; and

h. Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

COUNT VII
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE § 56, *ET SEQ*.
(On Behalf of Plaintiff Nathan Baxter and the California Subclass)

209. Plaintiff Nathan Baxter re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 98.

210. At all relevant times, Marker Group was a health care provider because they had the "purpose of maintaining medical information to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual."

211. Marker Group is a provider of healthcare within the meaning of Civil Code § 56.06(a) and maintains medical information as defined by Civil Code § 56.05.

212. Plaintiff Nathan Baxter and California Subclass Members provided their personal medical information to Marker Group.

213. At all relevant times, Marker Group collected, stored, managed, and transmitted the personal medical information of Plaintiff Nathan Baxter and California Subclass Members.

214. As a result of the Data Breach, Marker Group have misused, disclosed, and/or allowed third-parties to access and view the personal medical information of Plaintiff Nathan Baxter and California Subclass Members without their written authorization in accordance with the provisions of Civil Code §§ 56, *et seq*.

215. The hacker or hackers who committed the Data Breach obtained the personal medical information of Plaintiff Nathan Baxter and California Subclass Members, viewed it, and now have it available to them to sell to others bad actors or otherwise misuse.

216. As a further result of the Data Breach, the confidential nature of the medical information of Plaintiff Nathan Baxter and California Subclass Members was breached as a result of Defendant's negligence. Specifically, Marker Group knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access and view the PII and PHI of Plaintiff Nathan Baxter and California Subclass Members.

217. Defendant's misuse and/or disclosure of medical information regarding Plaintiff Nathan Baxter and California Subclass Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

218. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care, the personal medical information of Plaintiff Nathan Baxter and California Subclass Members was disclosed without written authorization.

219. By disclosing the PII and PHI of Plaintiff Nathan Baxter and California Subclass Members without their written authorization, Marker Group violated California Civil Code § 56, *et seq*., and their legal duty to protect the confidentiality of such information.

220. Marker Group also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

221. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, the personal medical information of Plaintiff Nathan Baxter and California Subclass Members was viewed by, released to, and disclosed to third-parties without Plaintiff's and California Subclass Members' written authorization.

222. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiff Nathan Baxter and California Subclass Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class, certifying the California Subclass for the claim under Cal. Civ. Code § 56, *et seq*., and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

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

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly

correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. purchasing credit monitoring and identity theft restoration services for Plaintiffs and Class Members for a period of ten years

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

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

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding

subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

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

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

D. For an award of damages, including actual, consequential, statutory, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: January 18, 2022

Respectfully Submitted,

/s/ Phillip Sanov
Phillip Sanov
TX Bar No. 17635950, SDTX ID No. 1148342
MORGAN & MORGAN
16225 Park Ten Place Suite 500
Houston, TX 77084

psanov@forthepeople.com

Jean S. Martin
Francesca Kester
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 559-4908
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

Paul Pennock
Jonathan M. Sedgh
MORGAN & MORGAN
850 3rd Ave, Suite 402
Brooklyn, NY 11232
Phone: (212) 738-6839
Fax: (813) 222-2439
ppennock@forthepeople.com
jsedgh@forthepeople.com

Christopher A. Seeger
SEEGER WEISS LLP
55 Challenger Rd
6th floor
Ridgefield Park, NJ 07660
(973) 639-9100
cseeger@seegerweiss.com

Stephanie O'Connor
DOUGLAS & LONDON, P.C.
59 Maiden Lane, 6th Fl.
New York, NY 10038
212-566-7500
212-566-5601 (fax)
sconnor@douglasandlondon.com

Attorneys for Plaintiffs and the Proposed Class