2/3/2022

RECEIVED

COMMONWEALTH OF MASSACHUSETTS

ESSEX, ss. SUPERIOR COURT DEPARTMENT

ELAINE LAFRATTA, individually and on behalf of all others similarly situated,

Plaintiff,

v.

MEDICAL HEALTHCARE SOLUTIONS, INC.,

Defendant.

Case No. 2277CV00102-C

CLASS ACTION COMPLAINT

Plaintiff Elaine LaFratta ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendant Medical Healthcare Solutions, Inc. ("MHS") and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against MHS for its failure to secure and safeguard her and at least 118,416 other individuals' private and confidential medical information ("PII/PHI"), including names, addresses, dates of birth, sexes, phone numbers, email addresses, Social Security numbers, driver's license/state ID numbers, financial account numbers, routing numbers, payment card numbers, card CVVs/expirations, diagnosis/treatment information, procedure types, provider names, prescription information, dates of service, medical record numbers, patient account numbers, insurance ID numbers, insurance group numbers, claim numbers, insurance plan names, provider ID numbers, procedure codes, treatment costs, and diagnosis codes.

2. MHS is a company that provides services for health care providers, such as billing and data analysis. The company purports to provide its clients with "INCREASED CASH FLOW, ELECTRONIC CLAIM SUBMISSION, CUSTOMIZED FINANCIAL REPORTS, STATE OF THE ART CODING PROCEDURES, and most importantly, CONFIDENTIALITY."[1]

3. Between October 1, 2021 and October 4, 2021, unauthorized individuals gained access to MHS's network systems and had access to and removed files from the system that contained the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. MHS owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. MHS breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its customers' patients' PII/PHI from unauthorized access and disclosure.

5. As a result of MHS's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all United States residents whose PII/PHI was exposed as a result of the Data Breach, which MHS learned of on November 19, 2021, and first publicly acknowledged on or about January 21, 2022, over two months after the breach was discovered.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, breach of express contract, breach of implied contract, and unjust enrichment, and

[1] *Medical Healthcare Services*, MEDICAL HEALTHCARE SOLUTIONS, INC., https://www.medicalhealthcaresolutions.com/services/ (last accessed Jan. 27, 2022)

seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff Elaine LaFratta is a Massachusetts resident, with a residence in Peabody, Massachusetts. She received medical treatment from a physician group that hired MHS for their medical billing. She received a letter from MHS notifying her that her PII/PHI may have been exposed in the Data Breach. Plaintiff LaFratta would not have obtained medical treatment from her provider had she known that her information would be transmitted to MHS and not adequately safeguarded by MHS.

8. Defendant Medical Healthcare Solutions, Inc. is a Massachusetts corporation with its corporate headquarters located at 300 Brickstone Square, Andover, MA 01810.

JURISDICTION AND VENUE

9. This Court has jurisdiction over the subject matter of this action because the amount in controversy exceeds the sum of $50,000.

10. This Court has personal jurisdiction over MHS because MHS is a corporation organized under the laws of Massachusetts and maintains a principal place of business in Massachusetts.

11. Venue is proper in Essex County because MHS's principal place of business is located in Essex County and Plaintiff resides in Essex County.

FACTUAL ALLEGATIONS

Overview of MHS

12. MHS offers a broad assortment of services to healthcare providers. The services that the company lists as providing include healthcare analytics, revalidation, electronic health records, revenue cycle management, and practice management consulting.[2]

13. In the regular course of its business, MHS collects and maintains the PII/PHI of the patients of health care providers for whom MHS provides billing and other services.

14. MHS's website contains a Privacy Policy which states, "Personal Health Information about an individual contained in the process of receiving and billing services from physicians, and reviewing reports and summaries of such services will be protected in accordance with the requirements and definitions of this Health Insurance Portability and Accountability Act."[3] The policy further states, "We are dedicated to observe all other state and federal laws relating to the transmission, storage and access to medical health care data and records."[4]

15. Plaintiff and Class members are, or were persons whose health care providers used MHS for billing services and entrusted MHS with their PII/PHI.

The Data Breach

16. Between October 1, 2021 and October 4, 2021, an unauthorized individual, or unauthorized individuals, gained access to MHS's network systems and removed certain files from MHS's computer systems. MHS did not discover that files were removed from its systems until over one month later, on November 19, 2021.

---

[2] *Id.*

[3] *Privacy Policy*, MEDICAL HEALTHCARE SOLUTIONS, INC., https://www.medicalhealthcaresolutions.com/company/privacy-policy/ (last accessed Jan. 27, 2022).

[4] *Id.*

17. MHS did not begin to notify government agencies or the public about the data breach until over two months after that, on or about January 21, 2022. The notice that MHS posted on its website states the information that was disclosed included:

> "[N]ame, address, date of birth, sex, phone number, email address, Social Security number, driver's license/state ID number, financial account number, routing number, payment card number, card CVV/expiration, diagnosis/treatment information, procedure type, provider name, prescription information, date of service, medical record number, patient account number, insurance ID number, insurance group number, claim number, insurance plan name, provider ID number, procedure code, treatment cost, and diagnosis code."[5]

18. In the notice, MHS "encourage[s]" individuals to "always remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors."[6]

19. Plaintiff's and Class members' PII/PHI was placed on the dark web by the cybercriminal group that took the PII/PHI from MHS's network.[7] Plaintiff and Class members are at an imminent risk of identity fraud now that their PII/PHI is available to any number of cybercriminals.

MHS Knew that Criminals Target PII/PHI

20. At all relevant times, MHS knew, or should have known, that the PII/PHI that it collected was a target for malicious actors. Despite such knowledge, MHS failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and

---

[5] *Notice of Cyber Incident*, MEDICAL HEALTHCARE SOLUTIONS, INC., https://www.medicalhealthcaresolutions.com/notice-of-cyber-incident/ (last accessed Jan. 27, 2022).

[6] *Id.*

[7] Dissent, *Hit by Conti Ransomware in October, Medical Healthcare Solutions Now Notifying Clients' Patients*, DATABREACHES.NET (Jan. 27, 2022), https://www.databreaches.net/hit-by-conti-ransomware-in-october-medical-healthcare-solutions-now-notifying-clients-patients/

Class members' PII/PHI from cyber-attacks that MHS should have anticipated and guarded against.

21. It is well known among companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers .... Many of them were caused by flaws in ... systems either online or in stores."[8]

22. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020, with over 40 million patient records exposed.[9] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[10]

23. PII/PHI is a valuable property right.[11] The value of PII/PHI as a commodity is measurable.[12] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory

---

[8] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[9] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Jan. 27, 2022).

[10] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Jan. 27, 2022).

[11] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible..."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[12] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

frameworks."[13] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[14] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

24. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated, thus becoming more valuable to thieves and more damaging to victims.

25. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[15] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[16] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[17]

---

[13] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[14] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[15] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[16] *Id.*

[17] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

26. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[18] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[19]

27. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[20] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[21]

28. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[22]

---

[18] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[19] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last accessed Jan. 27, 2022).

[20] *What Happens to Stolen Healthcare Data*, *supra* at n.15.

[21] *Id.*

[22] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An*

29. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

30. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[23]

31. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[24] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[25]

Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[23] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Jan. 27, 2022).

[24] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. 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. *Id.*

[25] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How*

32. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[26]

33. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[27]

34. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

35. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to

---

Can You Protect Yourself, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Jan. 27, 2022).

[26] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Jan. 28, 2021).

[27] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Jan. 27, 2022).

find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[28]

36. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[29] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[30] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[31] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[32]

37. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.

---

[28] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[29] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf

[30] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk…*, *supra* at n.18.

[31] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Jan. 27, 2022).

[32] *Id.*

- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[33]

38. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[34]

39. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

40. Plaintiff and Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii)

[33] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 28.
[34] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

41. This action is brought and may be properly maintained as a class action pursuant to Massachusetts Rule of Civil Procedure 23.

42. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

> All persons living in the United States whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.

43. Excluded from the Class is Medical Healthcare Solutions, Inc. and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

44. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

45. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. MHS reported to the Massachusetts Attorney General that approximately 118,417 Massachusetts residents' information was exposed in the Data Breach.

46. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether MHS had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether MHS failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

c. Whether an implied contract existed between Class members' health care providers and MHS, for which Class members are a third-party beneficiary, providing that MHS would implement and maintain reasonable security measures to protect and secure Class Members' PII/PHI from unauthorized access and disclosure;

d. Whether MHS breached its duties to protect Plaintiff's and Class members' PII/PHI; and

e. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

47. MHS engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

48. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiff and Class

members were injured by the same wrongful acts, practices, and omissions committed by MHS, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

49. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

50. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against MHS, so it would be impracticable for Class members to individually seek redress from MHS's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

51. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

52. MHS owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

53. MHS's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules"). Plaintiff and Class members are the persons that the HIPPA Privacy and Security Rules were intended to protect, and the harm that Plaintiff and Class members suffered is the type of harm the rules were intended to guard against.

54. MHS's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as MHS, of failing to employ reasonable measures to protect and secure PII/PHI. Plaintiff and Class members are the persons that the Section 5 of the FTCA was intended to protect, and the harm that Plaintiff and Class members suffered is the type of harm Section 5 of the FTCA intended to guard against.

55. MHS knew the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. MHS knew of the many data breaches that targeted companies that stored PII/PHI in recent years.

56. Given the nature of MHS's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, MHS should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

57. MHS breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

58. It was reasonably foreseeable to MHS that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

59. But for MHS's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

60. As a result of MHS's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks

justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II

BREACH OF EXPRESS CONTRACT

61. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

62. Plaintiff and Class members were the intended third-party beneficiaries of contracts entered into between MHS and Plaintiff's and Class members' health care providers. Plaintiff's and Class members' health care providers entered into contracts under which the health care providers paid monies to MHS and MHS provided billing services to the health care providers. Plaintiff and Class members were intended to benefit from these contracts, as they were the parties that were being billed for their health care providers' services. As evidenced by MHS's Privacy Policy, the safekeeping of Plaintiff and Class members' PII/PHI was necessary under the contracts.

63. MHS breached its obligations under the contracts between itself and Plaintiff's and Class members' health care providers by failing to implement and maintain reasonable security measures to protect and secure the PII/PHI of Plaintiff and Class members.

64. MHS's breach of the express contracts between itself, on the one hand, and Plaintiff's and Class members' health care providers, on the other hand, for which Plaintiff and Class members were intended third-party beneficiaries, directly caused the Data Breach.

65. Plaintiff and Class members were damaged by MHS's breach of express contracts because: (i) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) their PII/PHI was improperly disclosed to unauthorized individuals; (iii) the confidentiality of their PII/PHI has been breached; (iv) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT III

BREACH OF IMPLIED CONTRACT

66. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

67. In connection with receiving billing services, Plaintiff's and Class members' health care providers entered into implied contracts with MHS for which Plaintiff and Class members were intended third party beneficiaries.

68. Pursuant to these implied contracts, Plaintiff's and Class members' health care providers paid money to MHS and provided MHS with Plaintiff and Class members' PII/PHI. In exchange, MHS agreed to, among other things, and Plaintiff's and Class members' health care providers understood that MHS would: (1) provide billing services to the health care providers; (2) take reasonable measures to protect the security and confidentiality of

Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

69. The protection of PII/PHI was a material term of the implied contracts between Plaintiff's and Class members' health care providers, on the one hand, and MHS, on the other hand. Indeed, as set forth *supra*, MHS recognized the importance of data security and the privacy of the PII/PHI it collects in its Privacy Policy.

70. MHS breached its obligations under its implied contracts with Plaintiff's and Class members' health care providers in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

71. MHS's breach of its obligations in its implied contracts with Plaintiff's and Class members' health care providers directly resulted in the Data Breach and the injuries that Plaintiff and Class members have suffered from the Data Breach.

72. Plaintiff and Class members were damaged by MHS's breach of implied contracts because: (i) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) their PII/PHI was improperly disclosed to unauthorized individuals; (iii) the confidentiality of their PII/PHI has been breached; (iv) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT IV

UNJUST ENRICHMENT

73. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

74. This claim is pleaded in the alternative to the breach of express and implied contract claims.

75. Plaintiff and Class members conferred a monetary benefit upon MHS indirectly through their health care providers in the form of monies paid for health care services, which the health care providers used to obtain billing services from MHS.

76. MHS accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. MHS also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate the billing services.

77. As a result of MHS's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for and those payments without reasonable data privacy and security practices and procedures that they received.

78. MHS should not be permitted to retain the money belonging to Plaintiff and Class members because MHS failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

79. MHS should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against MHS as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent MHS from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: February 3, 2022

Respectfully submitted,

/s/ David Pastor
David Pastor (BBO 391000)
Email: dpastor@pastorlawoffice.com
PASTOR LAW OFFICE
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Tel: 617.742.9700
Fax: 617.742.9701

BEN BARNOW*
Email: b.barnow@barnowlaw.com
ANTHONY L. PARKHILL*
Email: aparkhill@barnowlaw.com
RILEY W. PRINCE*
Email: rprince@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504

**pro hac vice* to be submitted

CIVIL ACTION COVER SHEET

DOCKET NUMBER: 2277CV01026-C

Trial Court of Massachusetts 2
The Superior Court

COUNTY: Essex Superior Court (Salem) 2/3/2022

RECEIVED

Plaintiff	Elaine LaFratta	**Defendant:**	Medical Healthcare Solutions, Inc.
ADDRESS:	13 Rose Circle	ADDRESS:	300 Brickstone Square
	Peabody, MA 01960		Andover, MA 01810
Plaintiff Attorney:	David Pastor ~ Pastor Law Office, LLP	**Defendant Attorney:**	
ADDRESS:	63 Atlantic Avenue, 3d Floor	ADDRESS:	
	Boston, MA 02110		
	Email: dpastor@pastorlawoffice.com		
BBO:	391000	BBO:	

TYPE OF ACTION AND TRACK DESIGNATION (see instructions section below)

CODE NO.	TYPE OF ACTION (specify)	TRACK	HAS A JURY CLAIM BEEN MADE?
B99	Negligence arising out of data breach	F	☒ YES ☐ NO

*If "Other" please describe:

Is there a claim under G.L. c. 93A? ☐ YES ☒ NO

Is there a class action under Mass. R. Civ. P. 23? ☒ YES ☐ NO

STATEMENT OF DAMAGES PURSUANT TO G.L. c. 212, § 3A

The following is a full, itemized and detailed statement of the facts on which the undersigned plaintiff or plaintiff's counsel relies to determine money damages. For this form, disregard double or treble damage claims; indicate single damages only.

TORT CLAIMS

A. Documented medical expenses to date

1. Total hospital expenses
2. Total doctor expenses
3. Total chiropractic expenses
4. Total physical therapy expenses
5. Total other expenses (describe below)

Subtotal (1-5): **$0.00**

B. Documented lost wages and compensation to date

C. Documented property damages to date

D. Reasonably anticipated future medical and hospital expenses

E. Reasonably anticipated lost wages

F. Other documented items of damages (describe below)

TOTAL (A-F): **$0.00**

G. Briefly describe plaintiff's injury, including the nature and extent of injury:

Invasion of privacy and exposure to identity theft and fraud

CONTRACT CLAIMS

☐ This action includes a claim involving collection of a debt incurred pursuant to a revolving credit agreement. Mass. R. Civ. P. 8.1(a).

Item #	Detailed Description of Each Claim	Amount
1.		
	Total	

Signature of Attorney/Unrepresented Plaintiff: X /s/ David Pastor Date: February 3, 2022

RELATED ACTIONS: Please provide the case number, case name, and county of any related actions pending in the Superior Court.

CERTIFICATION PURSUANT TO SJC RULE 1:18

I hereby certify that I have complied with requirements of Rule 5 of the Supreme Judicial Court Uniform Rules on Dispute Resolution (SJC Rule 1:18) requiring that I provide my clients with information about court-connected dispute resolution services and discuss with them the advantages and disadvantages of the various methods of dispute resolution.

Signature of Attorney/Unrepresented Plaintiff: X /s/ David Pastor Date: February 3, 2022