IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF KENTUCKY

MARGARET GARRETT, individually and on behalf of all others similarly situated, Plaintiff, v. NORTON HEALTHCARE, INC., Defendant.	Case No. 3:23-cv-656-RGJ **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Margaret Garrett ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through undersigned counsel, brings this Class Action Complaint against Defendant Norton Healthcare, Inc. ("Norton" or "Defendant"), 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 Norton for its failure to secure and safeguard Plaintiff's and approximately 2.5 million other individuals' personally identifiable information ("PII") and personal health information ("PHI") (collectively, "PII/PHI"), including names in combination with one or more of the following: contact information, Social Security numbers, dates of birth, health information, insurance information, and medical identification number, and for certain persons, driver's license number, other government ID numbers, financial account numbers, and digital signatures.

2. Defendant is a Kentucky-based health system that offers a wide range of medical services throughout Kentucky, Southern Indiana, and beyond.

3. According to the "Notice of Security Incident"[1] ("Notice") published on Norton's website, on May 9, 2023, Norton "discovered that it was experiencing a cybersecurity incident, later determined to be a ransomware attack," "notified federal law enforcement and immediately began working with a respected forensic security provider to investigate and terminate the unauthorized access."[2]

4. Norton's investigation "determined that an unauthorized individual(s) gained access to certain network storage devices between May 7, 2023, and May 9, 2023," (the "Data Breach").[3]

5. Norton 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. Norton breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their patients' PII/PHI from unauthorized access and disclosure.

6. As a result of Norton's inadequate security measures 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 other individuals whose PII/PHI was exposed as a result of the Data Breach.

---

[1] *Notice of Security Incident*, NORTON HEALTHCARE, https://Nortonhealthcare.com/news/Norton-healthcare-network-update/ (last accessed Dec. 12, 2023).
[2] *Id.*
[3] *Id.*

7. Plaintiff, individually and on behalf of all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of Kentucky consumer protection statute. Plaintiff seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff

8. Plaintiff Margaret Garrett is and has been, at all relevant times, a resident and citizen of Crestwood, Kentucky. Plaintiff is a patient at Norton and has paid for and received medical services numerous times from Norton. Plaintiff provided PII/PHI to Norton, or otherwise had PII/PHI provided to Norton, in connection with receiving medical services from it. On December 13, 2023, Plaintiff received a letter from Norton dated December 8, 2023 notifying Plaintiff that Plaintiff's PII/PHI may have been exposed in the Data Breach.

Defendant

9. Defendant Norton Healthcare, Inc. is a non-profit corporation formed under the state laws of the commonwealth of Kentucky, with a principal place of business located at 4967 U.S. Highway 42, Suite 101, Louisville, Kentucky 40222.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than

Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

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

12. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Defendant's principal place of business is located in this District; Defendant maintains class members' PII/PHI in this District; and Defendant caused harm to class members residing in this District.

FACTUAL ALLEGATIONS

Overview of Norton Healthcare, Inc.

13. Norton Healthcare, Inc. is a Kentucky-based health system that touts itself as a "leader in serving adult and pediatric patients from throughout Greater Louisville, Southern Indiana, the commonwealth of Kentucky and beyond."[4] Norton is a not-for-profit hospital and health care system with five Louisville-based hospitals, three hospitals in Southern Indiana and one under construction in West Louisville scheduled to open in late 2024.[5]

14. Norton has more than 20,000 employees, over 1,750 medical providers and more than 3,000 total providers on its medical staff, making it Louisville's second largest employer. Norton claims to provide care at more than 430 locations throughout Kentucky and Southern Indiana, including at its five Louisville hospitals that have a total of 1,907 licensed beds, and the Southern Indiana hospitals that have a total of 347 licensed beds.[6]

[4] *About Us*, NORTON HEALTHCARE, https://Nortonhealthcare.com/about-us/ (last accessed Dec. 12, 2023).
[5] *Id.*
[6] *Id.*

15. Norton's hospitals provide inpatient and outpatient general care as well as specialty care, including heart, neuroscience, cancer, orthopedic, women's and pediatric services, and the health system includes 14 outpatient centers, 17 Norton Immediate Care Centers, nine Norton Prompt Care clinics and an expanded telehealth program.[7]

16. In the regular course of its business, Norton collects and maintains the PII/PHI of its patients, former patients, and other individuals to whom it is currently providing or previously provided medical and/or health-related services.

17. Norton requires patients to provide sensitive personal information prior to providing medical and/or health-related services. Upon information and belief, that information includes, per its Notice, *inter alia*, names in combination with contact information, Social Security numbers, dates of birth, health information, insurance information, and medical identification number, and for certain persons, driver's license number, other government ID numbers, financial account numbers, and digital signatures.

18. Norton provides on its website a "HIPAA" notice claiming "[w]e understand that medical information about the health of our patients is personal. We are committed to protecting patients' personal medical information,"[8] and a "Privacy Policy" in which it states, in pertinent part, that "Norton Healthcare is committed to protecting the privacy of visitors to our website, users of our mobile applications and users who subscribe to our mobile messaging campaigns."[9]

19. Upon information and belief, Norton also provides every patient with a HIPAA compliant disclosure form in which it represents that it will protect patients' PII/PHI.

---

[7] *Id*.
[8] *HIPAA*, NORTON HEALTHCARE, https://Nortonhealthcare.com/hipaa/ (last accessed Dec. 12, 2023).
[9] *Privacy Policy*, NORTON HEALTHCARE, https://Nortonhealthcare.com/privacy-policy/ (last accessed Dec. 12, 2023).

20. Plaintiff and class members are, or were, patients of or other persons affiliated with Norton, and/or received medical and/or health-related services from Norton, and entrusted Norton with their PII/PHI.

21. Plaintiff and class members, as former and current patients of or other persons affiliated with Norton, relied on these promises and on this well-established healthcare entity to keep their sensitive PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make certain only authorized disclosure of this information.

The Data Breach

22. In early December 2023, Norton published a "Notice of Security Incident" on its website after an unauthorized third party accessed certain computer systems in Norton's network. In its Notice, Norton explains:

> **WHAT HAPPENED?**
> On May 9, 2023, Norton Healthcare discovered that it was experiencing a cybersecurity incident, later determined to be a ransomware attack. Norton Healthcare notified federal law enforcement and immediately began working with a respected forensic security provider to investigate and terminate the unauthorized access. Our investigation determined that an unauthorized individual(s) gained access to certain network storage devices between May 7, 2023, and May 9, 2023, but **did not** access Norton Healthcare's medical record system or Norton MyChart. The nature and scope of the incident required time to analyze, a process that was substantially completed in mid-November.
>
> **WHAT INFORMATION WAS INVOLVED?**
> The impacted files contained personal information, primarily about patients, employees, and dependents. The information that may have been impacted varied from person-to-person, but could have included: name, contact information, Social Security Number, date of birth, health information, insurance information, and medical identification numbers. In some instances, the data may also have included driver's license numbers or other government ID numbers, financial account numbers, and digital signatures.[10]

[10] *See Notice of Security Incident*, n.1, *supra*.

23. Norton provides scant detail about the Data Breach and the steps that Norton is taking to address it. Norton's Notice does not provide the dates of Defendant's investigation, details of the root cause of the Data Breach, the vulnerabilities exploited, or details of the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class members, who retain a vested interest in ensuring that their PII/PHI remain protected.

24. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and class members of the Data Breach's critical facts. Without these details, Plaintiff's and class members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

25. Norton failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and class members, causing the exposure of PII/PHI, such as encrypting the information or deleting it when it is no longer needed.

26. The attacker accessed and acquired files in Norton's computer systems containing unencrypted PII/PHI of Plaintiff and class members, including names in combination with one or more of the following: contact information, Social Security numbers, dates of birth, health information, insurance information, and medical identification number, and for certain persons, driver's license number, other government ID numbers, financial account numbers, and digital signatures. Plaintiff's and class members' PII/PHI was accessed and stolen in the Data Breach.

27. As evidenced by the Data Breach's occurrence, the PII/PHI contained in Norton's system was not adequately protected from intrusions. Had the information been properly secured consistent with industry standard and best practices, the data thieves would have exfiltrated only unintelligible data.

Norton Knew That Criminals Target PII/PHI

28. At all relevant times, Norton knew, or should have known, its patients', Plaintiff's, and all other class members' PII/PHI was a target for malicious actors. Despite such knowledge, Norton failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and class members' PII/PHI from cyber-attacks that Norton should have anticipated and guarded against.

29. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as Social Security numbers ("SSNs") and medical information—is valuable and frequently targeted by criminals. Indeed, "[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."[11]

30. 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.[12] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[13]

---

[11] Dennis Green, et al., *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[12] Protenus, *2021 Breach Barometer*, PROTENUS.COM, available at https://www.protenus.com/resources/2021-breach-barometer (last accessed Dec. 6, 2023).

[13] Protenus, *2020 Breach Barometer*, PROTENUS.COM, available at https://www.protenus.com/resources/2020-breach-barometer (last accessed Dec. 6, 2023).

31. PII/PHI is a valuable property right.[14] The value of PII/PHI as a commodity is measurable.[15] "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 frameworks."[16] American companies spend many billions of dollars on acquiring personal data of consumers.[17] 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.

32. 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 and become more valuable to thieves and more damaging to victims.

33. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[18] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten

---

[14] *See* Marc van Lieshout, *The Value of Personal Data*, IFIP Advances in Information and Communication Technology. 457. 26-38 (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…"), available at https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[15] *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.

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

[17] 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/ (estimated to have spent over $19 billion in 2018).

[18] *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 (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

personal identifying characteristics of an individual."[19] 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.[20]

34. 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.[21] 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.[22]

35. John Riggi, the American Hospital Association National Advisor for Cybersecurity and Risk, said "foreign cyber gangs and spies" were testing the resilience of hospitals especially as hospitals began to fill up at the time because of the "tripledemic" including increased cases of RSV, flu and COVID-19.[23]

---

[19] *Id.*

[20] *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.

[21] 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 (last accessed Dec. 6, 2023).

[22] 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 Dec. 6, 2023).

[23] Dan Alexander, *Personal Data of 617,000 Patients Exposed in NJ Hospital Cyberattack*, NEW JERSEY 101.5 (Feb. 13, 2023), https://nj1015.com/personal-data-of-617000-patients-exposed-in-nj-hospital-cyberattack/.

36. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[24] Quoting Carbon Black's Chief Cybersecurity Officer, one 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."[25]

37. Consumers place a high value on the privacy of that data. 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."[26]

38. 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

39. Theft of PII/PHI is serious. The Federal Trade Commission ("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.[27]

---

[24] *What Happens to Stolen Healthcare Data*, *supra* at n. 18.

[25] *Id.*

[26] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available at https://www.jstor.org/stable/23015560?seq=1.

[27] *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 Dec. 6, 2023).

40. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[28] 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.[29]

41. 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.[30]

---

[28] 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*.

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

[30] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Dec. 12, 2023).

42. Identity theft is a very difficult 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.[31]

43. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new SSN, 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.

44. 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 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."[32]

45. 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."[33] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[34] 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

---

[31] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), available at https://www.idtheftcenter.org/.

[32] 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/.

[33] 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.

[34] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.22.

prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [35] 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."[36]

46. For these reasons, the information compromised in the Data Breach is significantly more valuable than the loss of basic financial information, because there, victims can cancel or close credit or debit card accounts. Upon information and belief, the information compromised by the Data Breach—for example, a Social Security number—is exceedingly difficult, if not impossible, to change.

47. 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.
- 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.

---

[35] *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 Dec. 12, 2023).

[36] *Id.*

- 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.[37]

48. 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.[38]

49. 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.

Norton Fails to Comply with Industry Standards

50. Cyber security experts routinely identify healthcare entities in possession of PII/PHI as being particularly vulnerable to cyberattacks because of the value of the information which they collect and maintain.

51. As a result, several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of PII/PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

---

[37] *See The Geography of Medical Identity Theft*, *supra* at n.33.

[38] 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.

Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

52. Norton failed to follow, enforce, or maintain the aforementioned best practices. Norton also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

Damages Sustained by Plaintiff and Class Members

53. 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) 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.

54. Plaintiff had a reasonable expectation of privacy in sensitive PII/PHI while receiving medical services. Plaintiff would not have agreed to have sensitive PII/PHI provided to and maintained by Norton had Plaintiff known that Norton would fail to adequately protect PII/PHI. Indeed, Plaintiff sought medical care through Norton with the reasonable expectation that Norton would keep PII/PHI secure and inaccessible to unauthorized parties. Plaintiff and class

members would not have obtained services from Norton had they known that Norton failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII/PHI from criminal theft and misuse.

55. Plaintiff and all other 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) 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/or (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.

56. As a result of Norton's failures, Plaintiff and class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII/PHI. Indeed, Plaintiff's damages are not merely speculative. Consequently, Plaintiff and class members now face a substantially increased risk of identity and medical theft that is plausibly imminent, considering the actual instances of fraud already suffered by other class members.

CLASS ALLEGATIONS

57. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

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

Nationwide Class

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

59. Alternatively, Plaintiff seeks to certify this action on behalf of the following state class:

Kentucky Class

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

60. Excluded from the classes are Norton 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).

61. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

62. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the 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.

63. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Norton reported that approximately 2.5 million individuals' information was exposed in the Data Breach.

64. 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 Norton 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 Norton 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 and Norton providing that Norton would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

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

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

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

66. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Norton, 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.

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

68. 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 Norton, so it would be impracticable for Class members to individually seek redress from Norton'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.

COUNT I
NEGLIGENCE

69. Plaintiff realleges and incorporates by reference paragraphs 1-68 as if fully set forth herein.

70. Norton 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.

71. Norton knew the risks of collecting and storing Plaintiff's and Class members' PII/PHI and the importance of maintaining secure systems. Norton knew of the many data breaches that targeted businesses that collect sensitive PII/PHI in recent years.

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

73. Norton 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.

74. It was reasonably foreseeable to Norton 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.

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

76. As a result of Norton's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other 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/or (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
NEGLIGENCE PER SE

77. Plaintiff realleges and incorporates by reference paragraphs 1-76 as if fully set forth herein.

78. Norton'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").

79. Norton'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 business, such as Norton, of failing to employ reasonable measures to protect and secure PII/PHI.

80. Norton violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and Class members' PII/PHI and not complying with applicable industry standards. Norton's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI

including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

81. Norton violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. Norton's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

82. Norton's violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

83. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

84. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were 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 practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and all other Class members as a result of the Data Breach.

85. It was reasonably foreseeable to Norton 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 release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

86. As a result of Norton's above-described wrongful actions, inaction, and want of ordinary care, and its negligence and negligence per se, 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, publication, and theft 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; (v) the continued risk to their PII/PHI which remains in Norton's possession; and (vi) 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. In addition, Class members already have suffered actual fraud, identity theft, and medical theft as alleged herein, demonstrating how imminent the threat of such fraudulent activity and damages are to all Class members.

COUNT III
BREACH OF FIDUCIARY DUTY

87. Plaintiff realleges and incorporates by reference paragraphs 1-86 as if fully set forth herein.

88. Plaintiff and Class members provided Norton their PII/PHI in confidence, believing that Norton would protect that information. Plaintiff and Class members would not have provided Norton with this information had they known it would not be adequately protected. Norton's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship

between Norton, on the one hand, and Plaintiff and Class members, on the other hand. In light of this relationship, Norton must act primarily for the benefit of their patients, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

89. Norton has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. Norton breached that duty by failing to properly protect the integrity of their systems containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that they collected.

90. As a direct and proximate result of Norton's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Norton's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach. In addition, upon information and belief, Class members already have suffered actual fraud, identity theft, and medical theft, demonstrating how imminent the threat of such fraudulent activity and damages are to all Class members.

COUNT IV
BREACH OF IMPLIED CONTRACT

91. Plaintiff realleges and incorporates by reference paragraphs 1-90 as if fully set forth herein.

92. In connection with receiving medical treatment, and/or health-related services Plaintiff and Class members entered into implied contracts with Norton.

93. Pursuant to these implied contracts, Plaintiff and Class members provided Norton with their PII/PHI. In exchange, Norton agreed to, among other things, among other things, and Plaintiff understood that Norton would: (1) provide medical treatment and/or health-related services to Plaintiff and Class members; (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.

94. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Norton, on the other hand. Indeed, as set forth *supra*, Norton recognized the importance of data security and the privacy of its patients' PII/PHI in, *inter alia*, its HIPAA notice and Privacy Policy. Had Plaintiff and Class members known that Norton would not adequately protect their patients' PII/PHI, they would not have received medical treatment or services from Norton.

95. Plaintiff and Class members performed their obligations under the implied contract when they provided Norton with their PII/PHI and paid—directly or through their insurers—for health care treatment, services, or health insurance premiums from Defendant.

96. Norton breached its obligations under its implied contracts with Plaintiff and Class members 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.

97. Norton's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and Class members have suffered from the Data Breach.

98. Plaintiff and Class members were damaged by Norton's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) 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; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) 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 V
UNJUST ENRICHMENT

99. Plaintiff realleges and incorporate by reference paragraphs 1-56 as if fully set forth herein.

100. This claim is pleaded in the alternative to the breach of implied contract claim.

101. Plaintiff and Class members conferred a monetary benefit upon Norton in the form of monies paid for healthcare services.

102. Norton accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Norton also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this information was used facilitate payment and make insurance claims.

103. As a result of Norton'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's and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

104. Norton should not be permitted to retain the money belonging to Plaintiff and Class members because Norton 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.

105. Norton 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.

COUNT VI
VIOLATIONS OF THE KENTUCKY CONSUMER PROTECTION ACT
(Ky. Rev. Stat. § 367.110, *et seq*.) ("KCPA")

106. Plaintiff realleges and incorporates by reference paragraphs 1-98 as if fully set forth herein.

107. This claim is pleaded on behalf of Plaintiff and the Kentucky Class.

108. Norton is "person" for purposes of the KCPA.

109. Defendant's conduct as alleged herein occurred in the conduct of trade.

110. The KCPA prohibits "unfair, false, misleading, or deceptive acts or practices in the conduct of any trade." Any person who "purchase or leases goods or services primarily for personal, financial, or household purposes and thereby suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by Ky. Rev. Stat. § 367.170, may bring an action under the Rule of Civil Procedure . . . ." Ky. Rev. Stat. § 267.220.

111. Norton violated the KCPA by concealing and failing to disclose data security vulnerabilities while touting that it values patient privacy. Norton had an ongoing duty to Plaintiff and the Kentucky Class to refrain from unfair and deceptive practices under the KCPA in the course of its business.

112. The practices of Norton, described above, violate the KCPA, for, *inter alia*, one or more of the following reasons:

a. Norton engaged in unconscionable commercial practices in failing to reveal material facts and information, which did, or tended to, mislead Plaintiff and the Kentucky Class members about facts that could not reasonably be known by the consumer;

b. Norton failed to reveal facts that were material to the transactions in light of representations of fact made in a positive manner;

c. Norton caused Plaintiff and the Kentucky Class members to suffer a probability of confusion and misunderstanding of legal rights, obligations and/or remedies by and through its conduct;

d. Norton failed to reveal material facts to Plaintiff and the Kentucky Class members with the intent that Plaintiff and the Kentucky Class members rely upon the omission;

e. Norton made material representations and statements of fact to Plaintiff and the Kentucky Class that resulted in Plaintiff and the Kentucky Class members reasonably believing the represented or suggested state of affairs to be other than what they actually were;

f. Norton intended that Plaintiff and other members of the Kentucky Class rely on its representations and omissions, so that Plaintiff and other Kentucky Class members would purchase Norton's services; and

g. Under all of the circumstances, Norton's conduct in employing these unfair and deceptive trade practices was malicious, willful, wanton and outrageous such as to shock the conscience of the community and warrant the imposition of punitive damages.

113. Plaintiff and the Kentucky Class suffered ascertainable loss and action damages as a direct and proximate result of Norton's concealments, misrepresentations, and/or failure to disclose material information.

114. Norton is liable to Plaintiff and the Kentucky Class members for damages in amounts to be proven at trial, including attorney's fees, costs, and punitive damages, as well as injunctive relief enjoining Defendants' unfair and deceptive practices, and any other relief deemed just and proper.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in Plaintiff's favor and against Norton 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 themselves and the Class, seeks appropriate injunctive

relief designed to prevent Norton 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: December 14, 2023

/s/ *John C. Whitfield, Esq.*

John C. Whitfield (KY Bar #76410)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
19 North Main Street
Madisonville, KY 42431
Phone: (270) 821-0656
Facsimile: (270) 825-1163
jwhitfield@milberg.com

Andrew W. Ferich*
Carlynne A. Wagner*
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel: (310) 474-9111
Fax: (310) 474-8585
aferich@ahdootwolfson.com
cwagner@ahdootwolfson.com

**Pro Hac Vice* application forthcoming

Counsel for Plaintiff and the Proposed Class

ClassAction.org