12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT DIVISION, CHANCERY DIVISION

VERONICA MARTIN, on behalf of herself individually and all others similarly situated, Plaintiff, v. COOK COUNTY HEALTH AND HOSPITALS SYSTEM and PERRY JOHNSON & ASSOCIATES, INC., Defendants.	Case No.: 2023CH09558 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

INTRODUCTION

Plaintiff Veronica Martin ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants Cook County Health and Hospitals System ("CCH") and Perry Johnson & Associates, Inc. ("PJA") (collectively, "Defendants") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against CCH for its failure to properly secure and safeguard Plaintiff's and Class Members' sensitive information, including their full names, dates of birth, , addresses, Social Security numbers ("personally identifiable information" or "PII") and medical and treatment information, which is protected health information ("PHI" and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, "Private Information").

2. Between approximately March 27, 2023, and May 2, 2023, an unauthorized third party gained access to PJA's network system and obtained files containing information about CCH's current and former patients (the "Data Breach").

3. Defendants collect and maintain the sensitive, non-public Private Information of former and current CCH patients, including Plaintiff and Class Members, without which Defendants could not perform their regular business activities. Defendants retain this information for at least many years and even after the patient-physician relationship has ended.

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

5. Defendants failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect its affiliates' patients' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

6. As a result of Defendants' inadequate security and breach of their 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 persons whose PII/PHI was exposed as a result of the Data Breach, which occurred between approximately March 27, 2023, and May 2, 2023.

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

8. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

9. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

10. Plaintiff Veronica Martin is and has been, at all relevant times, a resident and citizen of Chicago, Illinois.

11. Defendant Cook County Health and Hospitals System is an agency of the Cook County government. CCH may be served through Karen A. Yarbrough, Cook County Clerk, 118 N. Clark St., Chicago, IL 60602.

12. Defendant Perry Johnson & Associates Inc. is a Nevada corporation with its principal place of business at 1489 W Warm Springs Rd., Henderson, NV 89014. It may be served through its registered agent C T Corporation System, 701 S. Carson St., Suite 200, Carson City, NV 89701.

JURISDICTION AND VENUE

13. This Court has general personal jurisdiction over Defendant CCH, pursuant to 735 ILCS 5/2-209, because CCH because it is organized under the laws of this state and regularly does business or solicits business, engages in other persistent courses of conduct and/or derives substantial revenue from services provided to individuals in Cook County and in the State of Illinois, and expects or should reasonably expect to be in court here. This Court has personal jurisdiction over Defendant PJA, pursuant to 735 ILCS 5/2-209, because it transacts business within this state, makes or performs contracts within this state, and engages in other persistent courses of conduct and/or derives substantial revenue from services provided to individuals in Cook County and in the State of Illinois, and expects or should reasonably expect to be in court here.

14. This Court has subject matter jurisdiction over this matter pursuant to Ill. Const. 1970, art. VI, § 9.

15. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101 because CCH conducts its usual and customary business in this County and because a substantial portion of the events complained of occurred in this County.

BACKGROUND

Defendants' Businesses

16. CCH is an agency of Cook County, Illinois.[1] It is "one of the largest public health systems in the United States" and serves over 600,000 patients annually.[2]

17. CCH operates two hospitals, approximately 15 community health centers, and four pharmacies in Cook County.[3] CCH is also responsible for operating the Cook County Department of Public Health, Correctional Health Services (which provides health care to persons in Cook County Jail and the Juvenile Temporary Detention Center), and CountyCare (Cook County's Medicaid plan).[4]

18. Plaintiff and Class Members are current and former CCH patients.

19. As a condition of receiving medical services at CCH, CCH requires that its affiliates' patients, including Plaintiff and Class Members, entrust Defendants with highly sensitive personal information.

20. The information held by Defendants in their computer systems or those of their vendors at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

---

[1] *Cook County Health Strategic Plan 2023–2025,* COOK CNTY. HEALTH (2023), https://cookcountyhealth.org/wp-content/uploads/CCH_2022_Strategic_Plan-082922.pdf (last accessed Nov. 7, 2023) [hereinafter "*Strategic Plan*"].
[2] *Id.*
[3] *Locations,* COOK CNTY. HEALTH, https://cookcountyhealth.org/our-locations/ (last accessed Nov. 7, 2023).
[4] *Strategic Plan, supra* note 1.

21. Upon information and belief, Defendants made promises and representations to CCH's patients, including Plaintiff and Class Members, that the Private Information collected from them as a condition of obtaining medical services at CCH would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after it was no longer required to maintain it.

22. Indeed, in the online notice published to its website, CCH states that: "[w]e are required by law to protect the privacy of your health information and to provide you with this information and if you are affected, to notify you following a breach of unsecured protected health information."[5]

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

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

25. Defendants had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants has a legal duty to keep consumer's Private Information safe and confidential.

[5] *Notice of Privacy Practices,* COOK CNTY. HEALTH, https://cookcountyhealth.org/wp-content/uploads/2019_01.01.50-Notice-of-Privacy-Practices-English.pdf (last accessed Nov. 7, 2023).

26. Defendants had obligations created by FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

27. Defendants derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendants could not perform the services they provide.

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

The Data Breach

29. On or about September 29, 2023, CCH began sending Plaintiff and other victims of the Data Breach a Notice of Security Incident letter (the "Notice Letter"), informing them that:

30. Between approximately March 27, 2023, and May 2, 2023, "An unauthorized party gained access to the PJ&A network . . . and, during that time, acquired copies of certain files from PJ&A systems."[6] PJA informed CCH that the unauthorized party accessed files containing the PII/PHI of approximately 1.2 million CCH patients.[7]

31. According to the Notice of Data Security Incident posted on CCH's website, the "affected protected health information may have included names, and some combination of the following: dates of birth, addresses, medical record numbers, encounter numbers, medical

[6] *Cyber Incident Notice,* Perry Johnson & Assocs., https://www.pjats.com/downloads/Notice.pdf (last accessed Nov. 7, 2023) [hereinafter "*PJA Notice*"].
[7] *See Cook County Health Notice of Data Security Incident*, Cook Cnty. Health, https://cookcountyhealth.org/compliance-notice/ (last accessed Nov. 7, 2023) [hereinafter "*CCH Notice*"].

information, and dates/times of service."[8] CCH claims that approximately 2,600 patients' Social Security numbers were included in the Data Breach.[9]

32. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed. CCH also stored unencrypted Private Information on its vendors systems for prolonged periods of time despite warnings against doing so. Moreover, CCH failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive Private Information.

33. CCH's failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

34. Plaintiff further believes her Private Information and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

[8] *Id.*
[9] *Id.*

Defendants Acquire, Collect, and Store Plaintiff's and Class Members' Private Information

35. As a condition to obtain medical services from CCH, Plaintiff and Class Members were required to give their sensitive and confidential Private Information, directly or indirectly, to Defendants.

36. Defendants retain and store this information and derives a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class Members' Private Information, Defendants would be unable to perform their services.

37. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure. Moreover, CCH owed a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

39. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members or by CCH exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

40. Defendants' negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendants Knew, Or Should Have Known, of the Risk Because Healthcare Entities In Possession of Private Information Are Particularly Susceptible to Cyber Attacks.

41. Data thieves regularly target companies like Defendants' due to the highly sensitive information that they custody. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

42. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendants, preceding the date of the breach.

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

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

45. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential.

[10] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

46. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[11] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.[12]

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

48. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

---

[11] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Oct. 17, 2022).

[12] *See id.*

[13] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

49. Additionally, as companies became more dependent on computer systems to run their business,[14] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[15]

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

51. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

52. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s) and/or its vendor's server(s) and the significant number of individuals who would be harmed by the exposure of the unencrypted data.

53. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

54. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—

[14]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[15] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

55. As healthcare entities in possession of CCH's patients' and former patients' Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems, or those on which it transferred Private Information, were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Private Information

56. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] 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."[17]

57. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[18]

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

58. For example, Personal Information can be sold at a price ranging from $40 to $200.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

59. For example, Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[21]

60. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

61. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link

---

[19] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[20] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).
[21] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 17, 2022).

the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

62. Theft of PHI is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

63. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[23]

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

65. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[24]

---

[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Oct. 17, 2022).

[23] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

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

Defendants Fail to Comply with FTC Guidelines

69. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

70. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

[25] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

understand their network's vulnerabilities; and implement policies to correct any security problems.[26]

71. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[27]

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

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

74. These FTC enforcement actions include actions against healthcare entities, like Defendants. *See, e.g., In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's

[26] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).
[27] *Id.*

data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

75. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

76. Defendants failed to properly implement basic data security practices.

77. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to its affiliates' patients' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

78. Upon information and belief, Defendants were at all times fully aware of its obligation to protect the Private Information of CCH's patients. Defendants were also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendants Fail with HIPAA Guidelines

79. Defendants are covered entities under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"),

and 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.

80. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[28] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

83. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

84. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

85. HIPAA's Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

[28] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

86. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

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

88. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[29]

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

[29] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

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

91. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[30] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[31]

Defendants Fail to Comply with Industry Standards

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

93. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security,

[30] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[31] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

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

94. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

95. Defendants 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.

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

Defendants Breached Their Duties to Safeguard Plaintiff's and Class Members' Private Information

97. In addition to its obligations under federal and state laws, CCH owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing,

safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. CCH owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

98. CCH breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. CCH's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
b. Failing to adequately protect its affiliates' patients' Private Information;
c. Failing to limit the sharing of personal information on third party networks;
d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
e. Failing to sufficiently train its employees and vendors regarding the proper handling of CCH's patients' Private Information;
f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
g. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and,
h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

99. CCH negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access the unsecured and unencrypted Private Information.

100. Had CCH remedied the deficiencies in its information storage and security practices or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

COMMON INJURIES & DAMAGES

101. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

The Data Breach Increases Victims' Risk of Identity Theft

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

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

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

105. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

106. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

107. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

108. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[32]

109. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

110. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still

[32] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm,* Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance- finn/ (last visited on May 26, 2023).

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

111. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

112. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

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

114. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

115. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

116. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[33]

117. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[34]

118. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

Diminution of Value of Private Information

119. PII and PHI are valuable property rights.[35] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

---

[33] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[34] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[35] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

120. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[36]

121. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[37] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[38,39] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[40]

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

123. At all relevant times, CCH knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security systems were breached,

[36] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[37] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).
[38] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[39] https://datacoup.com/
[40] https://digi.me/what-is-digime/

including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

124. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

126. CCH was, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

127. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

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

129. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected

fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

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

131. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

PLAINTIFF MARTIN'S EXPERIENCE

132. Plaintiff is a current CCH patient.

133. In order to obtain medical services from CCH, she was required to provide her Private Information, directly or indirectly, to Defendants.

134. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff Martin's Private Information in their systems.

135. Plaintiff Martin is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

136. Upon information and belief, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties in the Data Breach, including her full name, Social Security number, date of birth, address, medical record number, encounter number, medical information, and dates/times of service.

137. As a result of the Data Breach, Plaintiff Martin made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the

legitimacy of the Data Breach upon receiving the Notice Letter. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

138. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

139. Plaintiff also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

140. The Data Breach has caused Plaintiff Martin to suffer fear, anxiety, and stress, which has been compounded by the fact that CCH has still not fully informed her of key details about the Data Breach's occurrence.

141. As a result of the Data Breach, Plaintiff Martin anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

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

142. Plaintiff Martin has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

143. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to 735 ILCS 5/2—801 *et seq.*

144. The Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class**
> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach (the "Class").
>
> **Illinois Subclass**
> All individuals residing in the state of Illinois whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach (the "Class").

145. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

146. Plaintiff reserves the right to amend the definitions of the Class and/or Illinois Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

147. Numerosity: The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. CCH indicated in the Notice of

Data Security Incident posted on its website that approximately 1.2 million patients' records were included in the Data Breach.[41]

148. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendants had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class Members;

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

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

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

[41] *CCH Notice, supra* note 14.

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

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

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

149. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

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

151. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

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

153. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

154. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

155. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

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

157. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

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

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

160. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches that targeted healthcare provides that collect and store PII/PHI in recent years.

161. Given the nature of Defendants' businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the

vulnerabilities to their systems or their third-party vendor's systems and prevented the Data Breach from occurring.

162. Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed 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.

163. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed 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.

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

165. As a result of Defendants' 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 suffer injury, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls,

texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

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

167. Defendants' 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").

168. Defendants' 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 CCH, of failing to employ reasonable measures to protect and secure PII/PHI.

169. Defendants' duties also arise from the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/45(a) which requires:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS. 530/45.

170. Additionally, under 815 ILCS 530/10, Defendants had a duty to "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach […] in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10.

171. Defendants violated HIPAA Privacy and Security Rules, Section 5 of the FTCA, and IPIPA by failing to, or contracting with companies that failed to, use reasonable measures to protect Plaintiff's and other Class members' PII/PHI, by failing to provide timely notice, and by not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI they obtain and store, 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.

172. Defendants' violation of IPIPA, HIPAA Privacy and Security Rules, and Section 5 of the FTCA constitutes negligence *per se*.

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

174. The harm occurring as a result of the Data Breach is the type of harm that IPIPA, 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 Class members as a result of the Data Brach.

175. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or

contracting with companies that failed 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.

176. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' violations of harm IPIPA, HIPAA Privacy and Security Rules, and Section 5 of the FTCA.

177. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

178. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein and brings this claim against CCH only ("Defendant" for the purposes of this count).

179. Plaintiff and Class members gave CCH their PII/PHI in confidence, believing that CCH would protect that information.

180. Plaintiff and Class members would not have provided CCH with this information had they known it would not be adequately protected. CCH's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between CCH and Plaintiff and Class members.

181. In light of this relationship, CCH must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

182. Due to the nature of the relationship between CCH and Plaintiff and Class members, Plaintiff and Class members were entirely reliant upon CCH to ensure that their PII/PHI was adequately protected. Plaintiff and Class members had no way of verifying or influencing the nature and extent of CCH's or its vendors data security policies and practices, and CCH was in an exclusive position to guard against the Data Breach.

183. CCH has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. They breached that duty by contracting with companies that failed to, properly protect the integrity of the system 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.

184. As a direct and proximate result of CCH's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs

associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

185. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein and brings this claim against CCH only ("Defendant" for the purposes of this count).

186. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with CCH.

187. Pursuant to these implied contracts, Plaintiff and Class members paid money to CCH, directly or through their insurance, and provided CCH with their PII/PHI. In exchange, CCH agreed to, among other things, and Plaintiff and Class members understood that CCH would: (1) provide 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.

188. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and CCH, on the other hand. Indeed, as set forth

supra, CCH recognized the importance of data security and the privacy of CCH's patients' PII/PHI. Had Plaintiff and Class members known that CCH would not adequately protect their PII/PHI, they would not have received healthcare or other services from CCH.

189. Plaintiff and Class members performed their obligations under the implied contract when they provided CCH with their PII/PHI and paid for healthcare or other services from CCH.

190. CCH 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, including by ensuring companies it contracts with implement and maintain reasonable security measures to protect 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.

191. CCH'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 all other Class members have suffered from the Data Breach.

192. Plaintiff and all other Class members were damaged by CCH'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; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased

risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

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

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

195. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid to CCH for healthcare services, which CCH used in turn to pay for PJA's services, and through the provision of their PII/PHI.

196. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate billing services and services provided to CCH.

197. As a result of Defendants' 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.

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

199. Plaintiff and Class members have no adequate remedy at law.

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

COUNT VI
Violations of The Illinois Consumer Fraud And Deceptive Business Practices Act, 815 ILCS 505/2, *et seq*.
(On Behalf of Plaintiff and the Illinois Subclass)

201. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein and brings this claim on behalf of herself and the Illinois Subclass (the "Class" for the purposes of this count).

202. Defendants offered and continues to offer healthcare or other related services in the State of Illinois.

203. Plaintiff and Class members purchased and received healthcare or other services from Defendants for personal, family, or household purposes.

204. Defendants engaged in unlawful and unfair practices in violation of the ICFA by failing to, or contracting with companies that failed to, implement and maintain reasonable security measures to protect and secure Plaintiff's and Class members' PII/PHI in a manner that complied with applicable laws, regulations, and industry standards.

205. Defendants make explicit statements to their patients that their PII/PHI will remain private.

206. Defendants' duties also arise from the Illinois Personal Information Protection Act, 815 ILCS 530/45(a) which requires:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS 530/45.

207. Defendants violated this duty by failing to, or contracting with companies that failed to, implement reasonably secure data security policies.

208. Defendants further violated the ICFA by failing to notify their current and former patients of the data breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10. Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. 815 ILCS 530/20.

209. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their PII/PHI. Further, Defendants' failure to adopt, or contracting with companies that failed to adopt, reasonable practices in protecting and safeguarding their patients' PII/PHI will force Plaintiff and Class members to spend time or money to protect against identity theft. Plaintiff and Class members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

210. As a result of Defendants' violations of the ICFA, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available

for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

PRAYER FOR RELIEF

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

A. For an order certifying the Class and Illinois Subclass, as defined herein, and appointing Plaintiff and her Counsel to represent the Class and Illinois Subclass;

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

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

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

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

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless CCH can provide to the

Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

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

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

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

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' networks are compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

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

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

xiii. requiring Defendants to implement a system of tests to assess their employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

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

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private

Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. for a period of 10 years, appointing a qualified an independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

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

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: November 21, 2023

Respectfully Submitted,

By: /s/ *Gary M. Klinger*

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Attorney for Plaintiff and the Proposed Class

Chancery Division Civil Cover Sheet
General Chancery Section **(12/01/20) CCCH 0623**

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

VERONICA MARTIN, on behalf of herself individually and all others similarly situated

Plaintiff

v.

COOK COUNTY HEALTH AND HOSPITALS SYSTEM and PERRY JOHNSON & ASSOCIATES, INC.

Defendant

Case No: _____

CHANCERY DIVISION CIVIL COVER SHEET
GENERAL CHANCERY SECTION

A Chancery Division Civil Cover Sheet - General Chancery Section shall be filed with the initial complaint in all actions filed in the General Chancery Section of Chancery Division. The information contained herein is for administrative purposes only. Please check the box in front of the appropriate category which best characterizes your action being filed.

Only one (1) case type may be checked with this cover sheet.

0005 ☐ Administrative Review
0001 ☑ Class Action
0002 ☐ Declaratory Judgment
0004 ☐ Injunction

0007 ☐ General Chancery
0010 ☐ Accounting
0011 ☐ Arbitration
0012 ☐ Certiorari
0013 ☐ Dissolution of Corporation
0014 ☐ Dissolution of Partnership
0015 ☐ Equitable Lien
0016 ☐ Interpleader

0017 ☐ Mandamus
0018 ☐ Ne Exeat
0019 ☐ Partition
0020 ☐ Quiet Title
0021 ☐ Quo Warranto
0022 ☐ Redemption Rights
0023 ☐ Reformation of a Contract
0024 ☐ Rescission of a Contract
0025 ☐ Specific Performance
0026 ☐ Trust Construction
0050 ☐ Internet Take Down Action (Compromising Images)

☐ Other (specify) _____

◉ Atty. No.: 6303726 ○ Pro Se 99500

Atty Name: Gary M. Klinger

Atty. for: Plaintiff Veronica Martin

Address: 227 W. Monroe Street, Suite 2100

City: Chicago State: IL

Zip: 60606

Telephone: 866-252-0878

Primary Email: gklinger@milberg.com

Pro Se Only: ☐ I have read and agree to the terms of the Clerk's Clerk's Office Electronic Notice Policy and choose to opt in to electronic notice from the Clerk's office for this case at this email address:

Email: _____