UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
FORT MYERS DIVISION

JOHANA MARTINEZ, individually and on behalf of all similarly situated persons,

Plaintiff, CASE NO.:

v.

NCH HEALTHCARE SYSTEM, INC.,

Defendant.
_____/

NCH'S NOTICE OF REMOVAL

Defendant, NCH HEALTHCARE SYSTEM, INC. ("NCH"), by and through undersigned counsel and pursuant to 28 U.S.C. §§ 1441, 1446 and Local Rule 4.02, hereby files this Notice of Removal of this action from the Twentieth Judicial Circuit in and for Collier County, Florida, Case Number 20-CA-000996, to the United States District Court for the Middle District of Florida, Fort Myers Division. In support of removal, NCH states as follows:

PRELIMINARY FACTS

1. On March 25, 2020, Plaintiff JOHANA MARTINEZ filed a civil *Class Action Complaint* ("Complaint") in the Twentieth Judicial Circuit in and for Collier County, Florida, Case Number 20-CA-000996, concerning an alleged data breach at NCH's medical facilities.

2. The Complaint is comprised of nine counts, all of which contain allegations that NCH violated numerous provisions of the Health Insurance Portability and

Accountability Act ("HIPAA"), 42 U.S.C. § 1320d, *et seq*, 45 C.F.R. 164.102, *et seq.* See Complaint, ¶¶ 40, 81, 92, 108, 114, 117, 120, 124, 129, 141, 144.

3. The Complaint also appears[1] to allege violations of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681, *et seq.*, and Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 41, *et seq*, as part of the allegations in Count I (Violation of Florida Deceptive and Unfair Trade Practices Act, § 501.201, *et seq.*) and Count III (Negligence *per se*). See Complaint, ¶¶ 86, 109.

4. NCH recognizes that there is no private cause of action under either the HIPAA or the FTCA,[2] and "a complaint alleging a violation of a federal statute as an element of a state cause of action, when Congress has determined that there should be no private, federal cause of action for the violation, does not state a claim 'arising under the Constitution, laws, or treaties of the United States.'" Merrell Dow Pharm. Inc. v. Thompson, 478 U.S. 804, 817 (1986) (quoting 28 U.S.C. § 1331).

5. However, removal is proper under 15 U.S.C. § 1681p of the FCRA, which states that "[a]n action to enforce any liability created under this subchapter may be brought in any appropriate United States district court." See also Lockard v. Equifax, Inc., 163 F.3d 1259, 1264 (11th Cir. 1998) (agreeing "that the language in the FCRA does not provide evidence that Congress intended to preclude removal").

6. Plaintiff alleges that NCH engaged in "unfair and deceptive practices" under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), and NCH was required

[1] NCH uses the term "appears" because Plaintiff does not define the acronyms she uses in the Complaint.
[2] See Sneed v. Pan Am. Hosp., 370 Fed. Appx. 47, 50 (11th Cir. 2010) (no private cause of action under HIPAA); Lingo v. City of Albany Dep't of Cmty. & Econ. Dev., 195 Fed. Appx. 891, 894 (11th Cir. 2006) (no private cause of action under FTCA).

under the FCRA "to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information." See Complaint, ¶¶ 85, 86; see also In re Brinker Data Incident Litig., 3:18-CV-686-J-32MCR, 2020 WL 691848, at *12 (M.D. Fla. Jan. 27, 2020) (recognizing failure to adequately secure personally identifiable information may qualify as an unfair practice under FTUDPA (citing Burrows v. Purchasing Power, LLC, No. 1:12-CV-22800-UU, 2012 WL 9391827, at *6 (S.D. Fla. Oct. 18, 2012))). Thus, the Court has federal question jurisdiction over Plaintiff's FDUTPA claim. See Lopez v. Chase Bank USA, N.A., 8:13-CV-1895-T-17MSP, 2014 WL 523475, at *2 (M.D. Fla. Feb. 8, 2014) (finding court had federal question jurisdiction under the FCRA where plaintiff raised state law claim alleging "Defendant is both a furnisher of information as well as a debt collector under 15 U.S.C. Sec. 1681 and also liable under Chapter 559, Florida Statutes").

7. The Complaint is the first occasion when federal questions of any nature have been alleged in this state court action. This pleading was served upon Defendant NCH on April 27, 2020.

FEDERAL JURISDICTION

8. "[A]ny civil action brought in a State court of which the district courts of the United States have original jurisdiction, may be removed by the defendant or the defendants, to the district court of the United States for the district and division embracing the place where such action is pending." 28 U.S.C. § 144l(a).

9. This Honorable Court has jurisdiction of this case pursuant to 28 U.S.C. § 1331 because Plaintiff has alleged a civil action arising under federal law on the face of the

Complaint. Metro. Life Ins. Co. v. Taylor, 481 U.S. 58, 63 (1987); Blab T.V. of Mobile, Inc. v. Comcast Cable Commc'ns, Inc., 182 F.3d 851, 854 (11th Cir. 1999).

10. Accordingly, the United States District Court for the Middle District of Florida, Fort Myers Division, is the proper venue for removal of this action.

SUPPLEMENTAL JURISDICTION

11. State law claims have been asserted by Plaintiff in the Complaint which arise out of the same nucleus of facts and circumstances forming the basis for the federal claims asserted in this suit. NCH therefore submits that an exercise of pendant jurisdiction by the Court pursuant to 28 U.S.C. § 1367, would be appropriate in this matter.

TIMELINESS OF REMOVAL

12. This Notice of Removal is timely because Plaintiff's Complaint was served on Defendant NCH on April 27, 2020, and is the first pleading which raises any federal questions arising under federal law. A copy of the Complaint filed in the state court proceedings is attached hereto along with all other documents which have been filed in the state court action.

STATE COURT RECORDS

13. Pursuant to Local Rule 4.02, NCH filed with this Notice of Removal a true and legible copy of all process, pleadings, orders, and other papers or exhibits of every kind that have been filed in the state court action as of the date of this filing.

14. NCH has not taken any substantial action in state court that could be construed as a waiver of its right to seek removal to federal court. See Yusefzadeh v. Nelson, Mullins, Riley & Scarborough, LLP, 365 F .3d 1244, 1246 (11th Cir. 2004); Del Rio v.

Scottsdale Ins. Co., 605CV14290RL19JGG, 2005 WL 3093434, at *3 (M.D. Fla. Nov. 18, 2005).

15. NCH will file a copy of this Notice of Removal with the Twentieth Judicial Circuit, as required by 28 U.S.C. § 1446(d).

CONSENT

16. Defense Counsel is assigned to represent the interests of Defendant NCH, and certifies that NCH consents to removal.

WHEREFORE, Defendant NCH HEALTHCARE SYSTEM, INC. respectfully requests that this Honorable Court enter an Order removing the entire case from the Twentieth Judicial Circuit in and for Collier County, Florida, to the United States District Court for the Middle District of Florida, Fort Myers Division.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on **May 27, 2020**, the foregoing was electronically filed with the Clerk of the Court by using the CM/ECF system, which will send a notice to all counsel of record.

Respectfully submitted,

/s/ Robin Horton Silverman

Vincent P. Beilman, III, Esq.
Florida Bar No. 23966
Ryan D. Schoeb, Esq.
Florida Bar No. 109257
Robin Horton Silverman, Esq.
Florida Bar No. 27934
WOOD, SMITH, HENNING & BERMAN LLP
1501 S. Church Ave, Suite 200
Tampa, FL 33629
Telephone: 813-422-6910
Fax: 813-425-6983
rschoeb@wshblaw.com
rhortonsilverman@wshblaw.com
klongo@wshblaw.com
Counsel for NCH

Filing # 105447084 E-Filed 03/25/2020 06:04:15 PM

IN THE CIRCUIT COURT OF THE TWENTIETH JUDICIAL CIRCUIT
IN AND FOR COLLIER COUNTY, FLORIDA
CIRCUIT CIVIL DIVISION

JOHANA MARTINEZ, individually and on behalf of all similarly situated persons,

Plaintiff,

v.

NCH HEALTHCARE SYSTEM, INC.

Defendant.

_____/

Civil Action No.

CLASS REPRESENTATION

Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff, JOHANA MARTINEZ, individually, and on behalf of all others similarly situated, brings this action against Defendant NCH HEALTHCARE SYSTEM, INC., ("Defendant" or "NCH") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") at Defendant's medical facilities. As a result of the Data Breach, Plaintiff and approximately 63,581 Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully

FILED: COLLIER COUNTY, CRYSTAL K. KINZEL, CLERK, 03/26/2020 12:02:07 PM

accessed due to the Data Breach. Information compromised in the Data Breach includes names, dates of birth, Social Security numbers, driver's license numbers, tribal identification numbers, financial account information, payment card information, medical histories, treatment information, medication or prescription information, beneficiary information, provider information, patient identification numbers, health insurance information, username and password information, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively the "Private Information").

2. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

3. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks, such as the phishing attack that obtained Defendant's employees' credentials. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

4. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

5. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

7. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

8. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

9. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

10. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to NCH's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

11. Plaintiff Johana Martinez is, and at all times mentioned herein was, an individual citizen of the State of Florida residing in the City of Naples.

12. Defendant NCH is a Florida not-for-profit health system with its principal place of business at 350 7th Street North, Naples, FL 34102.

JURISDICTION AND VENUE

13. The Court has subject matter jurisdiction over Plaintiff's claims under Florida Stat. § 26.012 and § 86.011. This Court has jurisdiction over this dispute because this complaint seeks damages in excess of $15,000.00 dollars, exclusive of interest and attorneys' fees

14. Venue is proper in Collier County pursuant to Florida Stat. § 47.011 and § 47.051 because Defendant NCH is headquartered and does business in this County, the cause of action accrued in this county, and NCH has an office for the transaction of its customary business in this county.

15. The Court has personal jurisdiction over Defendant because under Florida Stat. §48.193, Defendant personally or through its agents operated, conducted, engaged in, or carried on a business or business venture in Florida and/or had offices in Florida committed tortious acts in Florida, and because Defendant engaged in significant business activity within Florida.

DEFENDANT'S BUSINESS

16. The NCH Healthcare System is an alliance of more than 700 independent physicians and medical facilities in dozens of locations throughout Collier County and southwest Florida, including NCH Downtown Naples Hospital Campus, NCH North Naples Hospital Campus, NCH Physician Group, Naples Heart Institute and Marco Healthcare Center.

17. NCH Baker Hospital Downtown and NCH North Naples Hospital provide personalized care for over 40,500 patients a year in a two-hospital, 716 bed system.

18. The NCH Healthcare System offers advanced heart, cancer, obstetric, newborn, and pediatric care.

19. In the ordinary course of receiving treatment and health care services from NCH, patients are required to provide sensitive personal and private information such as:

- Names;
- Dates of birth;
- Social Security numbers;
- Driver's license numbers;
- Tribal identification numbers
- Financial account information;
- Payment card information;
- Medical histories;
- Treatment information;
- Medication or prescription information;
- Beneficiary information;
- Provider information;

- Address, phone number, and email address, and;
- Health insurance information.

20. NCH also gathers certain medical information about patients and creates records of the care they provide to them, including, but not limited to, the following:

- Patient identification numbers;
- Username and password information;
- Treatment information;
- Medication or prescription information, and;
- Provider information.

21. Additionally, NCH may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

22. All of NCH's employees, staff, entities, clinics, sites, and locations may share patient information with each other for various purposes without a written authorization, as disclosed in the NCH's Notice of Privacy Practices (the "Privacy Notice").[1]

23. The Privacy Notice is provided to every patient upon request and is posted on NCH's website.

24. Because of the highly sensitive and personal nature of the information NCH acquires and stores with respect to its patients, NCH promises, among other things: (A) "to maintain the privacy of your health information and to provide you with this Notice of our legal duties and privacy practices;" (B) "to abide by the terms of this Notice" [of Privacy Practices], and; (C) "to notify you in writing if we improperly use or disclose your health information in a

[1] https://www.nchmd.org/privacy-policy

manner that meets the definition of a "breach" under federal law. NCH further acknowledges that a breach generally occurs when health information about you is not encrypted and is accessed by, or disclosed to, an unauthorized person.[2]

THE CYBERATTACK AND DATA BREACH

25. On or around June 14, 2019, NCH became aware of suspicious activity related to its human resources, timekeeping, and payroll system.

26. NCH launched an investigation into this suspicious activity and determined that certain employees improperly opened or handled email or email attachments that were part of a phishing scheme.

27. Because of this, data thieves were able to use stolen credentials to gain access to the employees' payroll records and, worse, their employee email accounts.

28. Third party specialists undertook a manual and programmatic review of the entire contents of the relevant email accounts to determine what data was present as the investigation was not able to determine if any email was actually viewed.

29. On December 19, 2019, the review provided confirmation of the identities of those individuals who may have had information present within the email accounts under review.

30. The email accounts affected by this incident contained some combination of the following information: patient name, date of birth, driver's license number, tribal identification number, Social Security numbers, financial account information, payment card information, medical history, treatment information, medication or prescription information, beneficiary information, provider information, patient identification number, health insurance information, and/or username/email and password information.

[2] *Id.*

31. The Private Information contained in the emails, including health information, was not encrypted and was accessed by an unauthorized person(s).

32. Plaintiff believes her Private Information was stolen (and subsequently sold) in the Data Breach. Unsurprisingly, NCH could not rule out that Private Information was viewed or accessed in the Data Breach.[3]

33. Despite acknowledging that data thieves likely accessed Plaintiff's and the Class Members' Private Information, Defendant did not begin to notify affected patients until February 14, 2020, nearly eight months after the data breach was discovered.

34. NCH had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

36. NCH's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

37. In light of recent high profile data breaches at other healthcare companies, including, University of Washington Medicine (974,000 patients, December 2018), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Columbia Surgical Specialist of Spokane (400,000 patients, January 2019), UConn Health (326,629 patients, February 2019), Navicent Health (278,016

[3] https://www.nchmd.org/data-notice

patients, July 2018), NCH knew or should have known that its electronic records would be targeted by cybercriminals

38. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation 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, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

39. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in NCH's industry, including Defendant.

40. Defendant 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. NCH's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing PII and PHI;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process

to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption").

41. As the result of computer systems in dire need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, NCH negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

42. Accordingly, as outlined below, Plaintiff's and Class Members' daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft. Plaintiff and the Class Members also lost the benefit of the bargain they made with.

CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

43. Cyberattacks and data breaches at medical facilities like NCH are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

44. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[4]

45. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[5]

---

[4] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks

[5] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203

46. Cyberattacks are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.[6]

47. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA 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."[7]

48. The FTC recommends that identity theft 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 7 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.[8]

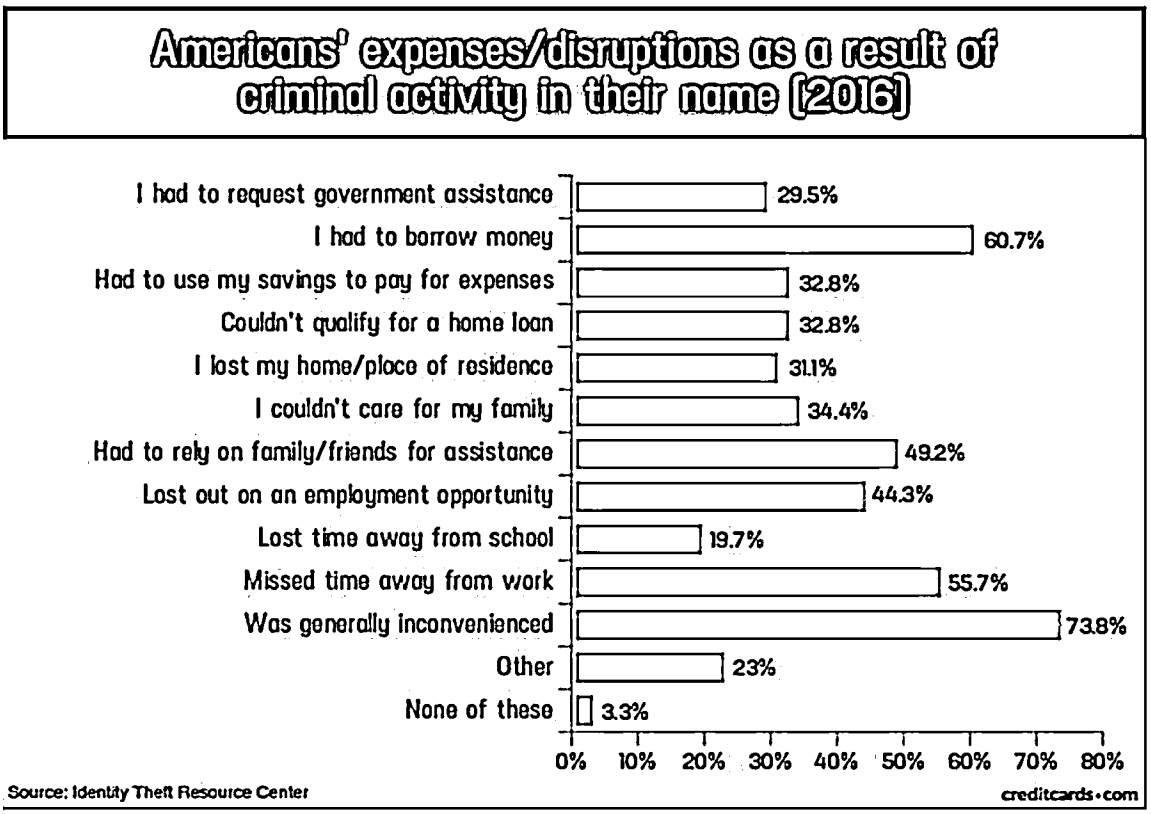
49. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

50. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give

---

[6] *Id.*
[7] *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 Apr. 12, 2019) ("GAO Report").
[8] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[9]



51. Moreover, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[10] Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this

[9] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).

[10] *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).

obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

52. Theft of PHI, in particular, 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."[11] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

53. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, 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.

See GAO Report, at p. 29.

54. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

---

[11] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 18, 2020).

55. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

56. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $50 and up.[12]

57. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

58. To date, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

59. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

60. Plaintiff's PII and PHI was compromised as a direct and proximate result of the Data Breach.

[12] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

61. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

62. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

63. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

64. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

65. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

66. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

67. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of NCH's computer

property and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

68. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse. Indeed, Defendant's own notice of data breach provides instructions to Plaintiff and Class Members about all the time that they will need to spend monitor their own accounts, or to establish a "security freeze" on their credit report.[13]

69. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

[13] https://www.nchmd.org/data-notice

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled, and;

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

70. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

71. Further, as a result of NCH's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

72. As a direct and proximate result of NCH's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

73. Plaintiff brings this suit on behalf of herself and a class of similarly situated individuals under Florida Rule of Civil Procedure 1.220, which is preliminarily defined as:

> All persons NCH identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

Excluded from the class are all employees, officers, and directors of Defendant, as well as any judges presiding over this matter and court personal assigned to this case.

74. **Numerosity**: The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, but are reported to be at least 63,581. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

75. **Commonality:** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

(a) Whether NCH violated state and federal laws by failing to properly store, secure, and dispose of Plaintiff's and Class Members' Personal Information;

(b) Whether NCH failed to employ reasonable and adequate data and cybersecurity measures in compliance with applicable state and federal regulations;

(c) Whether NCH acted willfully, recklessly, or negligently with regard to securing Plaintiff's and Class Members' Personal Information;

(d) How the Data Breach occurred;

(e) Whether NCH failed to timely notify Plaintiff and Class Members of the Data Breach;

(f) Whether Plaintiff and Class Members are entitled to restitution, damages, compensation, or other monetary relief; and

(g) Whether Plaintiff and Class Members are entitled to injunctive and declaratory relief necessary to secure their Personal Information from further intrusion and exposure.

76. Common sources of evidence may also be used to demonstrate NCH's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove NCH's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

77. **Typicality:** Plaintiff's claims are typical of the claims of the respective Class she seeks to represent, in that the named Plaintiff and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Class.

78. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Class and has retained attorneys well experienced in class actions and complex litigation as her counsel, including cases alleging consumer protection and data privacy claims arising from medical data breaches.

79. The Class also satisfies the criteria for certification under Florida Rule of Civil Procedure 1.220(b). Among other things, Plaintiff avers that the prosecution of separate actions by the individual members of the proposed Class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for NCH; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that NCH has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief described herein

appropriate with respect to the proposed Class as a whole; that questions of law or fact common to the Class predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiff further states that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Class will not be difficult.

80. Plaintiff and other members of the Class have suffered injury, harm, and damages as a result of NCH's unlawful and wrongful conduct. Absent a class action, NCH will continue to maintain Class Members' Personal Information that could be subject to future breaches due to lax or non-existent cybersecurity measures, and such unlawful and improper conduct should not go remedied. Absent a class action, the members of the Class will not be able to effectively litigate these claims and will suffer further harm and losses, as NCH will be allowed to continue such conduct with impunity and benefit from its unlawful conduct.

CLAIMS FOR RELIEF

COUNT I
Violation of Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, et seq.

81. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

82. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"). Fla. Stat. §§ 501.201, et seq. The express purpose of the FDUPTA is to "protect the consuming public . . . from those who engage in unfair methods of competition, or

unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

83. NCH's sale of goods and medical services at issue in this cause are "consumer transaction[s]" within the scope of the FDUTPA. Fla. Stat. §§ 501.201-501.213. Plaintiff is a "consumer[s]" as defined by the FDUTPA. Fla. Stat. § 501.203. NCH is engaged in trade or commerce within the meaning of the FDUTPA.

84. The FDUTPA declares as unlawful "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

85. The FDUPTA provides that "due consideration be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a)(1) of the Trade Commission Act." Fla. Stat. § 501.204(2). NCH's unfair and deceptive practices are likely to mislead -- and have misled -- the consumer acting reasonably under the circumstances. Fla. Stat. § 500.04; 21 U.S.C. § 343. As set forth above, NCH's Data Breach was a result of its substandard data and cybersecurity practices in violation of the state and federal requirements as set forth above.

86. Pursuant to the FCRA, HIPAA (42 U.S.C. § 1302d et seq.), the FTCA, and Florida law (Fla. Stat. § 456.057 and § 501.171), NCH was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information. NCH was also under an obligation expressly under Florida law, where NCH is headquartered and managed, to adequately protect Plaintiff's and Class Members' electronic Personal Information. Among other things, Florida requires NCH to (1) take reasonable measures to protect and secure data in electronic form containing PII; (2) take

reasonable measures to dispose of or destroy PII; and (3) provide notice to consumers and consumer reporting agencies subject to the FCRA when a data security incident occurs that compromises PII. Fla. Stat. §§ 501.171.

87. NCH has violated the FDUPTA by engaging in the unfair and deceptive practices described above, which offend public policies and are immoral, unethical, unscrupulous and substantially injurious to consumers. At all times material herein, NCH has failed to maintain adequate and reasonable data and cybersecurity protocols for Plaintiff's and Class Members' Personal Information in violation of state and federal laws and its own privacy practices and policies. NCH has also failed to take reasonable measures to destroy or dispose of Personal Information and timely notify its patients of the Data Breach in violation of Florida law.

88. Plaintiff has standing to pursue this claim because she has been injured by virtue of suffering a loss of privacy, money and/or property as a result of the wrongful conduct alleged herein. Plaintiff would not have purchased NCH's goods and services (or paid as much) had she known the truth about NCH's substandard and shoddy data and cybersecurity measures. Moreover, NCH will continue to maintain Plaintiff's and Class Members' Personal Information for the indefinite future, giving them a strong interest in ensuring such data is protected with state of the art, industry standards to prevent future data breaches. As a direct result of NCH's actions and omissions of material facts, Plaintiff and Class Members did not obtain the value of the goods and services for which they paid; were induced to pay for (or pay more for) medical goods and services that they otherwise would not have; and lost their ability to make informed and reasoned decisions about their medical treatment.

89. The damages suffered by Plaintiff and Class Members were directly and proximately caused by the deceptive, misleading and unfair practices of NCH, as described above.

90. Plaintiff and Class Members seek declaratory judgment that NCH's data security practices were not reasonable or adequate and caused the Data Breach under the FDUTPA, as well as injunctive relief enjoining the above described wrongful acts and practices of the NCH and requiring NCH to employ and maintain industry accepted standards for data management and security, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing. Fla. Stat. § 501.211(1).

91. Additionally, Plaintiff and Class Members make claims for actual damages, attorneys' fees and costs. Fla. Stat. §§ 501.2105, 501.211(2).

COUNT II
Negligence

92. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-80 as if fully set forth herein.

93. Plaintiff brings this claim individually and on behalf of the Class members.

94. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

95. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the type(s) of information that were compromised.

96. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

97. Defendant systematically failed to provide adequate security for data in its possession.

98. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

99. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

100. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

101. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

102. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding what type of Private Information has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

103. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

104. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

105. Plaintiff seeks the award of actual damages on behalf of herself and the Class.

106. In failing to secure Plaintiff's and Class Members' Private Information and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of herself and the Class.

107. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Defendant to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

COUNT III
Negligence *Per Se*

108. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-80 as if fully set forth herein. Plaintiff brings this claim on behalf of herself and the Class.

109. Pursuant to the FCRA, HIPAA (42 U.S.C. § 1302d et seq.), the FTCA, and Florida law (Fla. Stat. § 456.057 and § 501.171), NCH was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information.

110. NCH breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

111. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal Information in compliance with applicable laws would result in an unauthorized third-party gaining access to NCH's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Personal Information.

112. Plaintiff's and Class Members' Personal Information constitutes personal property that was stolen due to NCH's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

113. NCH's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Personal Information and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of NCH's conduct. Plaintiff and Class Members seek damages and other relief as a result of NCH's negligence.

COUNT IV
Breach of Express Contract

114. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-80 as if fully set forth herein. Plaintiff brings this claim on behalf of herself and the Class.

115. NCH provides medical services to Plaintiff and Class Members pursuant to the terms of its contracts, which all were a party to, including agreements regarding the handling of their confidential Personal Information in accordance with NCH's policies, practices, and applicable law. As consideration, Plaintiff and Class Members paid money to NCH and/or their insurers for medical services, and turned over their valuable PII and PIH to Defendant. Accordingly, Plaintiff and Class Members paid NCH to securely maintain and store their Personal

Information. NCH violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts.

116. Plaintiff and Class Members have been damaged by NCH's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
Breach of Implied Contract in Fact

117. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-80 as if fully set forth herein. Plaintiff brings this claim on behalf of herself and the Class.

118. NCH provides medical services to Plaintiff and Class Members. Plaintiff and Class Members also formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for medical goods and services from Defendant and by Defendant's performance of and sale of medical goods and services, regarding the handling of their confidential Personal Information in accordance with NCH's policies, practices, and applicable law. As consideration, Plaintiff and Class Members paid money to NCH and/or their insurers for medical services, and turned over their valuable PII and PIH to Defendant. Accordingly, Plaintiff and Class Members paid NCH to securely maintain and store their Personal Information. NCH violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts or agreements.

119. Plaintiff and Class Members have been damaged by NCH's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VI
Intrusion Upon Seclusion/Invasion of Privacy (Electronic Intrusion)

120. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

121. Plaintiff and Class Members maintain a privacy interest in their Personal Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above. Plaintiff and Class Members' Personal Information was contained, stored, and managed electronically in Defendant's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities, unique identification numbers, medical histories, and financial records that were only shared with Defendant for the limited purpose of obtaining and paying for healthcare, medical goods and services. Additionally, Plaintiff's and Class Members' Personal Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Personal Information for fraud, identity theft, and other crimes without their knowledge and consent.

122. NCH's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Personal Information is offensive to a reasonable person. NCH's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third parties permitted the physical and electronic

intrusion into Plaintiff's and Class Members' private quarters where their Personal Information was stored and disclosed private facts about their health into the public domain.

123. Plaintiff and Class Members have been damaged by NCH's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VII
Unjust Enrichment

124. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff brings this claim on behalf of the Class set forth above.

125. Plaintiff and Class Members conferred a benefit on NCH by paying for data and cybersecurity procedures to protect their Personal Information that they did not receive.

126. NCH has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to NCH's conduct alleged herein, it would be unjust and inequitable under the circumstances for NCH to be permitted to retain the benefit of its wrongful conduct.

127. Plaintiff and Class Members are entitled to full refunds, restitution and/or damages from NCH and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by NCH from its wrongful conduct. If necessary, the establishment of a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation may be created.

128. Additionally, Plaintiff and the Class Members may not have an adequate remedy at law against NCH, and accordingly plead this claim for unjust enrichment in addition to or, in the alternative to, other claims pleaded herein.

COUNT VIII
BREACH OF CONFIDENCE

129. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-80 as if fully set forth herein. Plaintiff brings this claim on behalf of herself and the Class.

130. At all times during Plaintiff's and Class Members' Interaction with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Personal Information.

131. As alleged herein and above, Defendant's relationship with Plaintiff's and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

132. Plaintiff and Class Members provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit Personal Information to be disseminated to any unauthorized parties.

133. Plaintiff and Class Members also provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect such Personal Information from unauthorized disclosure.

134. Defendant voluntarily received in confidence Plaintiff's and Class Members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

135. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiff's and Class Members' Personal Information, Plaintiff's and Class Members' Personal

Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

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

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

138. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Personal Information.

139. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching to prevent, detect, contest, and recover from medical fraud, financial fraud, and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information of patients in their continued

possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

140. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT IX
BREACH OF FIDUCIARY DUTY

141. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1-80 as if fully set forth herein. Plaintiff brings this claim on behalf of herself and the Class.

142. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship, as a consequence of the special relationship of trust and confidence that exists between patients (like Plaintiff and Class Members) and their medical care providers (like Defendant).

143. In light of their special relationship, Defendant has become the guardian of Plaintiff's and Class Members' Personal Information. Defendant has become a fiduciary, created by its undertaking and guardianship of patient Personal Information, to act primarily for the benefit of their patients, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' Personal Information and to timely notify them in the event of a data breach.

144. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to:

(a) properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' protected health information and other Personal Information;

(b) timely notify and/or warn Plaintiff and Class Members of the Data Breach.

(c) ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

(d) implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

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

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

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

(i) ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94);

(j) improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;

(k) effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5)

(l) design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c); and

(m) otherwise failing to safeguard Plaintiff's and Class Members' Personal Information.

145. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from

identity theft; (v) the continued risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect patient Personal Information in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

146. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on her own and behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action pursuant to Florida Rule of Civil Procedure 1.220, appointing Plaintiff as Class Representative, and the undersigned as Class Counsel;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Class has an effective remedy, including enjoining NCH from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

DATED: March 23, 2020

Respectfully submitted,

/s/ *Katherine Earle Yanes*
James E. Felman (FB# 775568)
Katherine Earle Yanes (FB# 159727)
Gus Centrone (FB# 30151)
KYNES, MARKMAN & FELMAN, P.A.
P.O. Box 3396
Tampa, FL 33601-3396
Telephone: (813) 229-1118
Facsimile: (813) 221-6750
Jfelman@kmf-law.com
Kyanes@kmf-law.com
Gcentrone@kmf-law.com

MASON LIETZ & KLINGER LLP
Gary E. Mason, Esq. (*pro hac vice to be submitted*)
David E. Lietz, Esq. (*pro hac vice to be submitted*)
5301 Wisconsin Avenue, NW, Suite 305
Washington, DC 20016
Telephone: 202-429-2290
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger (*pro hac vice forthcoming*)
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (312) 283-3814
Fax: (773) 496-8617
gklinger@masonllp.com

Attorneys for Plaintiff and the Proposed Class