CAUSE NO. _____

PATRICIA SMITH and SHARIE PERKINS, on behalf of herself and all others similarly situated,	§	**IN THE DISTRICT COURT OF**
***Plaintiffs*,**	§	
	§	**DALLAS COUNTY, TEXAS**
v.	§	
JDC HEALTHCARE MANAGEMENT LLC,	§	**_____ JUDICIAL DISTRICT**
***Defendant*.**	§	

PLAINTIFFS' ORIGINAL CLASS ACTION PETITION

Plaintiffs Patricia Smith and Sharie Perkins, ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Class Action Petition against Defendant JDC Healthcare Management LLC (hereinafter known as "JDC" or "Defendant"), a Texas limited liability company, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack against Defendant JDC that allowed a third party to access Defendant JDC's computer systems and data, resulting in the compromise of highly sensitive personal information belonging to hundreds of thousands of current and former patients of JDC (the "Data Breach"). Because of the Data Breach, Plaintiffs and more than a million other victims ("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, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive personal information.

2. Information compromised in the Data Breach includes names, dates of birth, Social Security numbers, driver's license numbers, financial information, health insurance information, medical information, and other protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") that Defendant collected and maintained (collectively the "Private Information").

3. Plaintiffs bring this class action lawsuit on behalf of those similarly situated 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 Plaintiffs and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party or precisely what specific type of information was accessed.

4. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to a cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

5. In addition, JDC and its employees failed to properly monitor the computer network and IT systems that housed the Private Information.

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

7. 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.

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

9. Plaintiffs 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.

10. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

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

12. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract; (iii)

negligence per se; (iv) breach of fiduciary duty; (v) intrusion upon seclusion/invasion of privacy and (vi) unjust enrichment.

II. PARTIES

Plaintiff Patricia Smith

13. Plaintiff Patricia Smith is a natural person, resident, and a citizen of the State of Texas. Defendant obtained and continues to maintain Plaintiff Smith's Private Information and owed her a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Smith would not have entrusted her Private Information to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff Smith's Private Information was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

14. Plaintiff received a notice letter from Defendant dated February 25, 2022 stating that Plaintiff's "name, billing/claims information, date of birth, doctor/medical professional name, group health insurance/subscriber number, individual health insurance subscriber number, other health insurance information, patient account number, Social Security number, and treatment information may have been accessed and/or acquired by an unauthorized individual."

Plaintiff Sharie Perkins

15. Plaintiff Sharie Perkins is a natural person, resident, and a citizen of the State of Indiana. Defendant obtained and continues to maintain Plaintiff Perkins' Private Information and owed her a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Perkins would not have entrusted her Private Information to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff Perkins' Private Information was compromised and disclosed as a result of Defendant's inadequate data security,

which resulted in the Data Breach.

16. Plaintiff received a notice letter from Defendant dated February 25, 2022 stating that Plaintiff's "name, billing/claims information, date of birth, doctor/medical professional name, group health insurance/subscriber number, individual health insurance subscriber number, other health insurance information, patient account number, Social Security number, and treatment information may have been accessed and/or acquired by an unauthorized individual."

Defendant JDC Healthcare Management LLC

17. Defendant JDC Healthcare Management LLC is a Texas professional association with its principal place of business at 3030 LBJ Freeway, Suite 1400, Dallas, TX 75231. Defendant JDC may be served through its Registered Agent, Cogencv Global Inc., 1601 Elm Street, Suite 4360, Dallas, TX, 75201.

III. JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action because the contract between Plaintiffs and Defendant was established in Dallas (Dallas County), Texas. Plaintiffs have been damaged in a sum within the jurisdictional limits of this Court. Pursuant to Texas Rule of Civil Procedure 47, Plaintiffs seek monetary relief over $1,000,000.00. Plaintiffs reserve the right to amend their petition during and/or after the discovery process.

19. This Court has personal jurisdiction over Defendant because it is a resident of the State of Texas.

20. Venue is proper in this County under Tex. Civ. Prac. & Rem. Code § 15.002 because a substantial part of the events or omissions giving rise to the claim occurred in this County.

21. Upon information and belief, each Plaintiffs' respective individual damages are less than $75,000.

22. Upon information and belief, at least two-thirds of the Class (defined *infra*) are residents of Texas.

IV. DEFENDANT'S BUSINESS

23. Defendant JDC Healthcare Management LLC, doing business as Jefferson Dental Orthodontics, provides dental care services, including preventative and cosmetic dentistry, bad breath, teeth cleaning and whitening, dental fillings and implants, bridges, gum disease, tooth extraction, root canal, and emergency care services in the States of Texas and Oklahoma. JDC has approximately seventy treatment locations and offices in Texas and at least two treatment locations in Oklahoma.

24. In the ordinary course of receiving dental care services from Defendant JDC, each patient and employee must provide (and Plaintiffs did provide) Defendant JDC with sensitive, personal, and private information, such as their:

a. Name, address, phone number, and email address;

b. Date of birth;

c. Social Security number;

d. Demographic information;

e. Driver's license or state or federal identification;

f. Information relating to the individual's dental and medical history;

g. Insurance information and coverage; and

h. Banking and/or credit card information.

25. Defendant also creates and stores medical/dental records and other protected health information for its patients, including records of treatments and diagnoses.

26. Upon information and belief, JDC's HIPAA Privacy Policy is provided to every

patient prior to receiving treatment and upon request.

27. Defendant JDC agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including HIPAA.

28. The patient information held by Defendant JDC in its computer system and network included the Private Information of Plaintiffs and Class Members.

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

30. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

31. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

V. THE CYBERATTACK

32. Publicly, Defendant has disclosed that cybercriminals accessed its network on July 27, 2021. According to Defendant, it did not learn about this until August 9, 2021.

33. Defendant has publicly stated that the Private Information "involved in the Data Breach includes "clinical information, demographic information (including Social Security numbers, driver's license numbers, and dates of birth), health insurance information, and financial information." Defendant has further admitted that this Private Information was "accessed and/or acquired" by cybercriminals.

34. It has been reported that approximately 1,026,820 Texas residents had their PII and PHI exposed in the Data Breach.[1]

35. The Private Information contained in the files accessed by hackers was not encrypted.

36. It is likely the Data Breach was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

37. Upon information and belief, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiffs and the Class Members.

38. Because of the Data Breach, data thieves were able to gain access to and hold hostage Defendant's IT systems and, were able to compromise, access, and acquire the protected Private Information of Plaintiffs and Class Members.

39. Defendant had obligations created by HIPAA, contract law, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

40. Defendant'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.

41. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[2] Of the 1,862 recorded

[1] https://www.hipaajournal.com/jdc-healthcare-management-data-breach-affects-more-than-1-million-texans/ (last visited April 18, 2022).

[2] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[3] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[4]

42. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, 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), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

43. Indeed, cyberattacks 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, "[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."[5]

44. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[6]

45. Therefore, the increase in such attacks, and attendant risk of future attacks, was

[3] *Id*.
[4] *Id*.
[5] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Jan. 25, 2022).
[6] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

46. 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.

47. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The 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; understand their network's vulnerabilities; and implement policies to correct any security problems.[7] 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.[8]

48. The FTC further recommends that companies not maintain PII 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.

49. The FTC has brought enforcement actions against businesses for failing to

[7] 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 June 15, 2021).
[8] *Id*.

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.

50. These FTC enforcement actions include actions against healthcare providers like Defendant. *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 data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

51. Defendant failed to properly implement basic data security practices.

52. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

53. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

54. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

55. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all

employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

56. 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; and training staff regarding critical points.

57. Defendant 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.

58. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Conduct Violates HIPAA Standards of Care and Evidences Its Insufficient Data Security

59. HIPAA requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

60. Covered entities (including Defendant JDC) must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

61. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

62. A Data Breach such as the one Defendant experienced is also 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

63. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[9]

64. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate JDC failed to comply with safeguards and standards of care mandated by HIPAA regulations.

[9] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.

VI. DEFENDANT'S NEGLIGENT ACTS AND BREACH

65. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant'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;

b. Failing to adequately protect patients' Private Information;

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

d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

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 protected health information to allow 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);

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

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 definition of encryption);

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

p. Failing to adhere to industry standards for cybersecurity.

66. As the result of antivirus and malware protection software in dire need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks like the ransomware intrusion here, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access, and hold hostage, JDC's IT systems, which contained unsecured and unencrypted Private Information.

67. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

68. Data breaches at healthcare providers like Defendant are especially problematic because the breaches can negatively impact the overall daily lives of individuals affected by the attack.

69. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment because of the disruption of service.

70. This leads to a deterioration in the quality of overall care patients receive at facilities

affected by data breaches.

71. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[10]

72. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[11]

73. Similarly, data breach incidents cause patients issues with receiving care that rise above the level of mere inconvenience. The issues that patients encounter as a result of such incidents include, but are not limited to:

a. rescheduling their medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. inability to access their medical records.[12]

74. 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

[10] *See* Nsikan Akpan, Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart- attacks (last visited Jan. 25, 2022).

[11] *See* Sung J. Choi et al., Cyberattack Remediation Efforts and Their Implications for Hospital Quality, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Jan. 25, 2022).

[12] *See, e.g.,* Lisa Vaas, Cyberattacks Paralyze, and Sometimes Crush, Hospitals, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals// (last visited Jan. 25, 2022); Jessica David, Data Breaches Will Cost Healthcare $4B in 2019. Threats Outpace Tech, Health IT Security (Nov. 5, 2019), https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech - :~:text=November 05, 2019 - Healthcare data,per each breach patient record (last visited Jan. 25, 2022).

"substantial costs and time to repair the damage to their good name and credit record."[13]

75. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, taking over victims' identities in order to engage in illegal financial transactions under the victims' names. 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.

76. 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 (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.[14]

77. Identity thieves use stolen personal information such as Social Security numbers

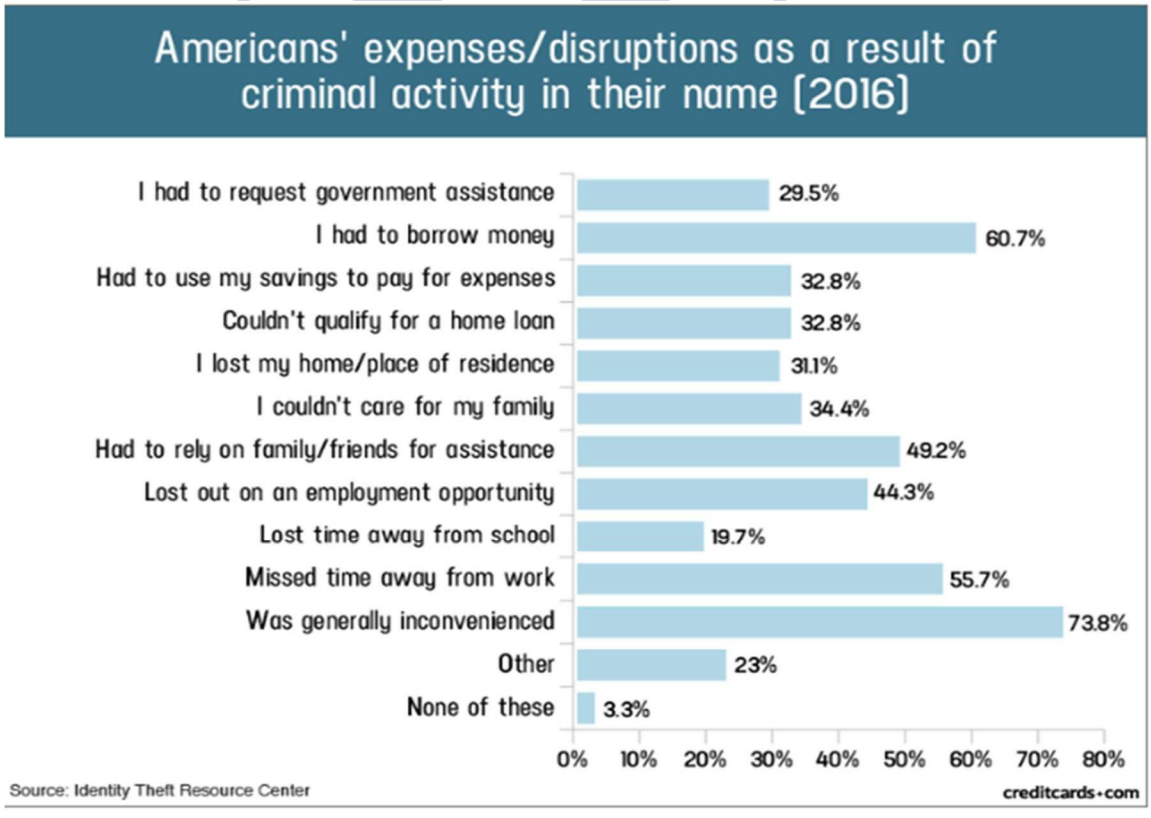
[13] *See* U.S. Gov. Accounting Office, GAO-07-737, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" (GOA, 2007). Available at https://www.gao.gov/new.items/d07737.pdf. (last visited Jan. 25, 2022).

[14] *See* IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 25, 2022).

for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

78. 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 the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

79. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[15]



[15] *See* Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. (last visited Jan. 25, 2022).

80. Moreover, theft of Private Information results in the loss of a valuable property right.[16]

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

82. 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."[17]

83. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and 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.

84. 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.

85. According to the U.S. Government Accountability Office, which conducted a study

[16] *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).

[17] *See* Federal Trade Commission, What to Know About Medical Identity Theft, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft identity-theft (last visited Jan. 25, 2022).

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.

86. 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.

87. 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 Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

88. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

89. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[18] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

90. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[19] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social

---

[18] *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 Jan. 25, 2022).

[19] Identity Theft and Your Social Security Number, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 25, 2022).

Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[20] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number 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.

91. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

92. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

93. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

94. Medical information is especially valuable to identity thieves.

95. 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.[21] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[22]

96. Because of the value of its collected and stored data, the medical industry has

[20] *Id*. at 4.
[21] *See* Omri Toppol, Email Security: How You Are Doing It Wrong & Paying Too Much, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last visited Jan. 25, 2022).
[22] *See* Vaas, Cyberattacks, *supra*, n. 28.

experienced disproportionally higher numbers of data theft events than other industries.

97. For this reason, Defendant knew or should have known about these dangers and strengthened its data security 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.

VII. PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

98. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has merely offered Plaintiffs and Class Members fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach. Signing up for this service requires Plaintiffs and Class Members to forfeit time that could otherwise be spent making money or enjoying life. Moreover, following the expiration of the 12-month subscription, Plaintiffs and Class Members will be required to pay for credit monitoring services out of their own pocket.

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

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

101. Plaintiffs 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 target such schemes more effectively to Plaintiffs and Class

Members.

102. Plaintiffs 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.

103. Plaintiffs and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of their Private Information, a form of property that JDC obtained from Plaintiffs and Class Members; (b) violation of their privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

104. Plaintiffs and Class Members were also injured by and suffered benefit-of-the-bargain damages from this Data Breach. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of JDC's computer system and network and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

105. Plaintiffs 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. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

106. Moreover, Plaintiffs 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 Private Information is not accessible online and that access to such data is password protected.

Plaintiff Smith's Experience

107. Plaintiff received medical care and treatment at JDC Healthcare in the past. Upon information and belief, during the course of the visits, she was presented with standard medical forms to complete prior to her service that requested her PII and PHI, including HIPAA and privacy disclosure forms.

108. As part of her care and treatment, and as a requirement to receive Defendant's services, Plaintiff entrusted her PII, PHI, and other confidential information such as name, address, Social Security number, medical and treatment information, and health insurance information to JDC Healthcare with the reasonable expectation and understanding that JDC Healthcare would take at a minimum industry standard precautions to protect, maintain, and

safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have used JDC Healthcare's services had she known that JDC Healthcare would not take reasonable steps to safeguard her sensitive PII and PHI.

109. Plaintiff also provided her credit card and banking information for payment of prescription and copays directly to JDC Healthcare or to its billing vendors.

110. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

111. Plaintiff has spent a significant number of hours reviewing her bank accounts, contacting her bank, and contacting other businesses, and will continue to spend valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

112. Plaintiff suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights;(c) the likely theft of her PII and PHI; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

113. As a result of the Data Breach, Plaintiff has also suffered emotional distress as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of identity theft and fraud. Plaintiff is very concerned about identity

theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

114. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

Plaintiff Perkins' Experience

115. Plaintiff received medical care and treatment at JDC Healthcare in the past. Upon information and belief, during the course of the visits, she was presented with standard medical forms to complete prior to her service that requested her PII and PHI, including HIPAA and privacy disclosure forms.

116. As part of her care and treatment, and as a requirement to receive Defendant's services, Plaintiff entrusted her PII, PHI, and other confidential information such as name, address, Social Security number, medical and treatment information, and health insurance information to JDC Healthcare with the reasonable expectation and understanding that JDC Healthcare would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have used JDC Healthcare's services had she known that JDC Healthcare would not take reasonable steps to safeguard her sensitive PII and PHI.

117. Plaintiff also provided her credit card and banking information for payment of prescription and copays directly to JDC Healthcare or to its billing vendors.

118. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

119. Plaintiff has spent a significant number of hours reviewing her bank accounts, contacting her bank, and contacting other businesses, and will continue to spend valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

120. Plaintiff suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights;(c) the likely theft of her PII and PHI; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

121. Subsequent to the Data Breach, an unidentified person attempted to set up a Wells Fargo account in Plaintiff Perkins' name without her knowledge or consent.

122. Moreover, subsequent to the Data Breach, Plaintiff also experienced an increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages which she did not receive before the breach. Plaintiff believes these calls and messages were targeted for purposes of committing a social engineering attack.

123. As a result of the Data Breach, Plaintiff has also suffered emotional distress as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of identity theft and fraud. Plaintiff is very concerned about identity

theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

124. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

VIII. CLASS ACTION ALLEGATIONS

125. Plaintiffs bring this action on behalf of themselves and all other persons similarly situated.

126. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

> **All persons whose Private Information was compromised as a result of the July - August 2021 Data Breach, for which JDC provided notice on or about February 25, 2022 (the "Class").**

127. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

128. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 42(a), (b)(2), and (b)(3).

129. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiffs at this

time, but JDC has provided notice to HHS that the number is not less than 1,000,000 individuals.

130. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was per se negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

o. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

131. Typicality. Plaintiffs claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach.

132. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

133. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The

common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

134. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

135. Defendant has 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.

136. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

137. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

IX. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

138. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

139. Defendant JDC required Plaintiffs and Class Members to submit non-public personal information in order to obtain healthcare/dental services and/or employment.

140. By collecting and storing this data in JDC's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property-and Class Members' Private Information held within it-to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

141. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

142. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant JDC and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

143. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. §

164.530(c)(l). Some or all of the healthcare, dental, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

144. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

145. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

146. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

147. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry, and even more so, because Defendant JDC experienced another significant data breach in February 2020.

148. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

149. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

150. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

151. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

152. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

153. When Plaintiffs and Class Members provided their Private Information to Defendant JDC in exchange for Defendant JDC's services and/or employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

154. Defendant JDC solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

155. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

156. Plaintiffs and Class Members paid money to Defendant or provided labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

157. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

158. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

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

160. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

161. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

162. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

163. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and All Class Members)

164. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

165. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

166. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs and Class Members' Private Information.

167. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, 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." See definition of encryption at 45 C.F.R. § 164.304.

168. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

169. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

170. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

171. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that they failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

172. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOURTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

173. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

174. In light of the special relationship between Defendant JDC and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

175. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of JDC's relationship with its patients, in particular, to keep secure their Private Information.

176. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

177. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs and Class Members' Private Information.

178. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

179. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

180. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs 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 Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and 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 Private 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 the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

181. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH COUNT
INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(On Behalf of Plaintiffs and All Class Members)

182. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

183. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts§ 652B (1977).

184. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

185. Defendant's conduct as alleged above intruded upon Plaintiffs and Class Members' seclusion under common law.

186. By intentionally failing to keep Plaintiffs and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

187. Defendant knew that an ordinary person in Plaintiffs or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

188. Defendant invaded Plaintiffs and Class Members' right to privacy and intruded into Plaintiffs and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

189. Defendant intentionally concealed from and delayed reporting to Plaintiffs and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

190. The conduct described above was at or directed at Plaintiffs and the Class Members.

191. As a proximate result of such intentional misuse and disclosures, Plaintiffs and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

192. In failing to protect Plaintiffs and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seeks an award of damages on behalf of himself and the Class.

SIXTH COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and All Class Members)

193. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

194. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of implied contract count, the second count listed in this Complaint.

195. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

196. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

197. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and

services that were the subject of the transaction and have their Private Information protected with adequate data security.

198. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

199. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

200. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

201. Defendant failed to secure Plaintiffs and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

202. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

203. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

204. Plaintiffs and Class Members have no adequate remedy at law.

205. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and 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; (f) the continued risk to their Private 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 Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

206. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

207. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

X. JURY TRIAL DEMANDED

208. Plaintiffs demand a trial by jury on all claims so triable.

PRAYER FOR RELIEF

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

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

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

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

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

iii. requiring Defendant to delete, destroy, and purge the personal identifying

information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

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

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

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

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

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

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

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

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with

additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

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

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

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

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

xvi. requiring Defendant to implement logging and monitoring programs sufficient

to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's 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, nominal, statutory, 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.

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

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

ATTORNEYS FOR PLAINTIFFS

***Pro Hac Vice Forthcoming**