IN THE UNITED STATES DISTRICT COURT

DISTRICT OF COLORADO

Natalie Willingham, *on behalf of herself and all others similarly situated*, Plaintiff, v. Professional Finance Company, Inc., Defendant.	Case No. **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Natalie Willingham ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Professional Finance Company, Inc. ("PFC" or "Defendant"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information and protected health information ("PHI") that Defendant collected, stored, and maintained on behalf of Plaintiff and Class Members, including, without limitation, first and last name, address, accounts receivable balance and information regarding payments made to accounts, and, in some cases, date of birth, Social Security number, and health insurance and medical treatment information (collectively, "personally identifiable

information" or "PII"),[1] for failing to comply with industry standards to protect information systems that contain that PII and PHI, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII and PHI had been accessed by an unauthorized third party. Plaintiff also alleges that Defendant failed to provide timely, accurate, and adequate notice to Plaintiff and Class Members of precisely what types of information was unencrypted and subject to access by and/or potentially in the possession of unknown third parties. Plaintiff seeks, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised, to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future, to destroy information no longer necessary to retain for the purposes that the information was first obtained from Class Members, and to provide a sum of money sufficient to provide to Plaintiff and Class Members identity theft protective services for their respective lifetimes as Plaintiff and Class Members as Plaintiff and Class Members are now and forever subject to an increased risk of identity theft due to the conduct of Defendant as described herein.

2. Defendant is a debt collector or "accounts receivable management" company located in Greeley, Colorado.[2] Defendant employs approximately 126 people and has an annual revenue of over $27 million.[3] According to Defendant's website, "[t]housands of national clients rely on [Defendant] to recover their receivables and manage their early out self-pay programs."[4]

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[2] https://www.pfcusa.com/about-us/ (last visited July 6, 2022).

[3] https://www.datanyze.com/companies/professional-finance-company/72616125 (last visited July 7, 2022).

[4] https://www.pfcusa.com/about-us/ (last visited July 6, 2022); *see also* Marianne Kolbasuk McGee, *Vendor's Ransomware Attack Hits Over 600 Healthcare Clients,* GOVINFOSECURITY.COM (Jul. 5, 2022), https://www.govinfosecurity.com/vendors-ransomware-attack-hits-over-600-healthcare-clients-a-19506.

Defendant represents itself as one of the "nation's leading debt recovery agencies," and states that its client list includes many healthcare providers, retailers, financial organizations, and government agencies.[5]

3. On or about July 1, 2022, Defendant posted a *Notice of Cybersecurity Incident* ("Website Notice") onto its website.[6] In the Website Notice, Defendant revealed that on or about February 26, 2022, PFC "detected and stopped" a ransomware attack in which an "unauthorized third party accessed and disabled some of PFC's computer systems" (the "Data Breach").[7]

4. Following the Data Breach, Defendant states that it engaged a third-party forensic specialist and determined that 657 of its healthcare provider clients ("Covered Entities") were affected.[8] A list of the Covered Entities affected by the Data Breach is attached as Exhibit 2.

5. According to the Website Notice, Defendant reviewed the data (stored on Defendant's systems) that was accessed in the Data Breach and confirmed that the data contained PII and PHI, such as names, addresses, accounts receivable balances, information regarding payments made to accounts, and, for some individuals, birth dates, Social Security numbers, health insurance information, and medical treatment information.[9]

6. Plaintiff and Class Members entrusted an extensive amount of their PII and PHI to Defendant directly or indirectly through Defendant's customers. Defendant retains this information on its systems.

7. As a result of the Data Breach, Plaintiff and likely millions of 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

[5] https://www.hipaajournal.com/657-healthcare-providers-affected-by-ransomware-attack-on-professional-finance-company/ (last visited July 7, 2022).
[6] Exhibit 1 ("Website Notice").
[7] *Id*.
[8] Exhibit 2 ("Covered Entities List"), *available at* https://bit.ly/CoveredEntitiesPFC.
[9] *See* Ex. 1.

the attack and the substantial and ongoing risk of identity theft.

8. As a condition of providing services related to healthcare, medical treatment and services, processing medical claims, sending bills, and providing collection services for treatment, Defendant requires that its customers entrust it with PII and PHI. Plaintiff and Class Members entrusted Defendant with, and allowed Defendant to gather, highly sensitive information relating to their health and other matters. When Plaintiff and Class Members provided their PII and PHI to Defendant, either directly or indirectly through Defendant's customers, Plaintiff and Class Members did so in confidence, and they had the legitimate expectation that Defendant will respect their privacy and act appropriately.

9. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff' and Class Members' PII and PHI from unauthorized disclosure.

10. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI.

11. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals. Defendant asserts that it understands the importance of protecting such information and that "[d]ata security is one of PFC's highest priorities."[10]

12. Upon information and belief, at the time of the Data Breach, the PII and PHI of Plaintiff and Class Members were accessible from the internet, regardless of whether there were any security mechanisms that Defendant mistakenly believed would safeguard the PII and PHI from unauthorized access via the internet.

[10] Ex. 1.

13. PFC promotes itself as being HIPAA-compliant; specifically, on its website, PFC states that it is "[f]ully compliant with all regulations, specifically FDCPA (Fair Debt Collection Practices Act), TCPA (Telephone Consumer Protection Act), and HIPAA (Health Insurance Portability and Accountability Act)."[11] By holding itself out to customers as such, Defendant adopted HIPAA regulations as its governing standard of conduct.

14. Upon information and belief, at the time of the Data Breach, none of the PII and PHI had been encrypted; further, at the time of the Data Breach, the PII and PHI included information that Defendant no longer had a reasonable need to maintain.

15. Despite knowing of the Data Breach since at *least* February 26, 2022, Defendant did not disclose the Data Breach to Plaintiff and Class Members until July 1, 2022.

16. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers. Plaintiff and Class Members are currently suffering and for the rest of their lifetimes will suffer the significant and concrete risk that their identities will be (or already have been) misused.

17. This PII and PHI was subject to unauthorized access and/or acquisition due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members.

18. Plaintiff brings this action on behalf of all persons whose PII and PHI was accessed, acquired, and/or misappropriated as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the PII and PHI of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

[11] https://www.pfcusa.com (last visited July 7, 2022).

19. Additionally, as a result of Defendant's failure to follow contractually-agreed upon, federally-prescribed, industry standard security procedures, Plaintiff and Class Members received only a diminished value of the services Defendant was to provide.

20. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up 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 PII and PHI.

21. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

22. Defendant has a duty to safeguard and protect customer information entrusted to it and could have prevented this theft had it limited the customer information received from its business associates, including medical records unrelated to debt collection, and employed reasonable measures to ensure its systems that contained millions of individuals' PII and PHI were secure from threats like ransomware attacks.

23. As the result, the PII and PHI of Plaintiff and Class Members was accessed and/or

acquired by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

24. Plaintiff Natalie Willingham is a resident of Hayes County, Texas and a citizen of the State of Texas.

25. Defendant Professional Finance Company, Inc. is a corporation organized under the laws of Colorado, and its United States headquarters and principal place of business is located at 5754 W. 11th St., Ste 100, Greeley, Colorado 80634.

26. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

27. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

28. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class, defined below, many of which are citizens of a different state than Defendant. Defendant PFC is a citizen of Colorado, where it maintains its principal place of business.

29. This Court has personal jurisdiction over Defendant because Defendant is found within this District and conducts substantial business in this District.

30. Venue is proper in this Court under 28 U.S.C. § 1391 because Defendant is headquartered and resides in this judicial district, its senior officers are located in this judicial district and Defendant regularly transacts business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

IV. FACTUAL ALLEGATIONS

Background

31. Defendant PFC is an "accounts receivable management company" located in Greeley, Colorado.[12] Defendant is one of the "nation's leading debt recovery agencies," and its client list includes many healthcare providers, retailers, financial organizations, and government agencies.[13]

32. Defendant employs approximately 126 people and has an annual revenue of over $27 million.[14]

33. According to Defendant's website, "[t]housands of national clients rely on [Defendant] to recover their receivables and manage their early out self-pay programs."[15]

34. Defendant's customers include the 657 Covered Entities whose patient information was impacted by the Data Breach. To its customers and their patients, PFC promotes itself as being HIPAA-compliant; specifically, on its website, PFC states that it is "[f]ully compliant with all regulations, specifically FDCPA (Fair Debt Collection Practices Act), TCPA (Telephone Consumer Protection Act), and HIPAA (Health Insurance Portability and Accountability Act)."[16] By holding itself out to customers as such, Defendant adopted HIPAA regulations as its governing

[12] https://www.pfcusa.com/about-us/ (last visited July 6, 2022).
[13] https://www.hipaajournal.com/657-healthcare-providers-affected-by-ransomware-attack-on-professional-finance-company/ (last visited July 7, 2022).
[14] https://www.datanyze.com/companies/professional-finance-company/72616125 (last visited July 7, 2022).
[15] https://www.pfcusa.com/about-us/ (last visited July 6, 2022); *see also* Marianne Kolbasuk McGee, *Vendor's Ransomware Attack Hits Over 600 Healthcare Clients,* GOVINFOSECURITY.COM (Jul. 5, 2022), https://www.govinfosecurity.com/vendors-ransomware-attack-hits-over-600-healthcare-clients-a-19506.
[16] https://www.pfcusa.com (last visited July 7, 2022).

standard of conduct.

35. As a condition of providing services to its customers and their patients, Defendant collected and stored some of Plaintiff's and Class Members' most sensitive and confidential person and medical information, including, without limitation, names, addresses, accounts receivable balances, information regarding payments made to accounts, birth dates, Social Security numbers, health insurance information, and medical treatment information. This includes information that is static, does not change, and can be used to commit myriad financial and healthcare-related crimes.

36. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII and PHI.

37. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from involuntary disclosure to third parties.

Defendant's Privacy Policies

38. On its customer-facing website, Defendant has a posted Privacy Policy, last updated February 25, 2020 (the "Privacy Policy").[17]

39. The Privacy Policy states "[y]our privacy is important to PFC. Our Privacy Policy covers how PFC collects, uses, maintains and discloses your personal information."

40. The Privacy Policy also discusses the types of information PHC collects and the reasons that it might use that information. It states, in part:

> In order to provide and improve our services, we collect personal information. Most of the information we have is provided to us by the creditor and/or collected directly through the use of our services, emails, web applications, and phone calls.

[17] Exhibit 3.

> Here are some examples of the types of personal information PFC may collect and how we use it:
>
> - When an account is transferred to PFC the creditor provides a variety of information which may include, but is not limited to: full name, date of birth, social security number, phone number, address, email address, account number, original creditor, current creditor, balance, payment history.
> - We may collect any information that you provide to us directly whether you contact us by phone, email, sms, web applications, or any other channel. For example, when you access PFC web applications and fill out a form or sign up for a payment plan and provide information such as your first and last name, email address, mailing address, phone number, credit card information and/or other personal identifying information.
> - When you access PFC emails or our web applications we may collect a variety of information and store it in log files, including, but not limited to Internet Protocol (IP) address, browser type and language, Internet service provider (ISP), type of computer, operating system, date/time stamp, user interface interaction data (such as, but not limited to, any mouse clicks or navigation on our emails and web applications), uniform resource locator (URL) information (showing where you came from or where you go to next), email open rates, credit card, bank account information.
>
> ***Using Personal Information***
>
> We use personal information to properly identify the specific consumers for whom we provide our services, to provide and improve our services, to analyze trends, administer our web applications, learn about user behavior on our emails and web applications, to comply with state, federal and local laws and to demonstrate compliance with those laws.

41. The Privacy Policy also provides instances when PFC might share PII and PHI with third-parties. It states:

> We only share personal information with a limited number of third party service providers who help us provide our services, including, but not limited to, payment processing, mailing, information verification, managing and enhancing customer data, improving our product and services. When we share information, we require those third parties to handle it in accordance with relevant laws. We also only share the minimum amount of information necessary for the

particular third party to assist us in providing our service.[18]

42. Defendant lists a number of instances when it might share or disclose the PII and PHI entrusted to it without permission, none of which are applicable here.[19]

43. The Privacy Policy also states, under *Integrity and Retention of Personal Information* that "PFC will retain your personal information for the period required to fulfill our services, meet our contractual obligations, and as required by law."

44. Further, under *How We Protect Your Information*, Defendant states "PFC is serious about data security."[20] With respect to the data stored on its systems, Defendant states:

> We seek to implement the best practices in data collection, storage, processing, and security to protect against unauthorized access and disclosure. PFC protects your personal information during transit using encryption such as Transport Layer Security (TLS) and at rest using encryption such as AES 256. When your personal data is stored by PFC, we use computer systems with limited access housed in facilities using physical security measures.[21]

45. Defendant's Privacy Policy distinguishes between the security of data stored on its systems and the security of data *in transit* between Defendant and its customers or Defendant and any other third party.

46. Defendant acknowledges that "no data transmission over the internet or any wireless network can be guaranteed to be 100 percent secure," however, the circumstances related to transit or transmission are not applicable here.

47. According to Defendant's own admissions, the Data Breach involved PII and PHI that was "at rest" and stored on Defendants internal systems, as discussed below.

48. Finally, Defendant's payment portal, accessible through its debt collection website

[18] *Id.*
[19] *See id.*
[20] *Id*.
[21] *Id*.

"pfccollects.com" has a "Privacy Policy."[22] It states, in part:

> Professional Finance Company has created this security and privacy statement in order to document and communicate its commitment to doing business with the highest ethical standards and appropriate internal controls. This Internet Privacy Policy describes the privacy policies applicable to Professional Finance Company's U.S. Internet websites www.ProfessionalFinanceCompany.com, www.pfccollects.com, and www.paypfc.com. Professional Finance Company has implemented physical, electronic, and procedural security safeguards to protect against the unauthorized release of or access to personal information. To further safeguard this information, our employees are asked to sign an acknowledgment of Professional Finance Company's Standards of Employee Conduct, which includes the Company Equipment and Office Guidelines and the General Technology Use Guidelines. Employees are subject to disciplinary action up to and including termination of employment if they fail to follow signed acknowledgments.[23]

49. It also states that to access the Defendant's website for "purposes of reviewing an account or making payment to PFC, personally identifiable information (PII) *must be provided*."[24] It continues to state that the types of "PII that may be collected includes: (1) A first and last name. (2) A home or other physical address, including street name and name of a city or town. (3) An e-mail address. (4) A telephone number. (5) A social security number. (6) A date of birth. (7) An employer. (8) A spouse's name and contact information."[25]

The Data Breach

50. On or about July 1, 2022, Defendant posted the Website Notice.[26] It read, in part, as follows:

> Professional Finance Company, Inc. ("PFC") is notifying individuals whose information may have been involved in a recent network security incident. PFC is an accounts

[22] The Payment Portal Privacy Policy is no longer available, however, a web-archived snapshot dated March 29, 2019 is available at https://web.archive.org/web/20190329055426/https://pfccollects.com/p/privacy-policy.html (last visited July 7, 2022). Further references to the Payment Portal Privacy Policy are made in reference to this web-archived snapshot.
[23] *Id*.
[24] *Id*. (emphasis added).
[25] *Id*.
[26] Ex. 1.

receivable management company that provides assistance to various organizations (including healthcare providers).

On February 26, 2022, PFC detected and stopped a sophisticated ransomware attack in which an unauthorized third party accessed and disabled some of PFC's computer systems. PFC immediately engaged third party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. Federal law enforcement was also notified. The ongoing investigation determined that an unauthorized third party accessed files containing certain individuals' personal information during this incident. PFC notified the respective healthcare providers on or around May 5, 2022. This incident only impacted data on PFC's systems. The list of healthcare providers can be viewed here: https://bit.ly/CoveredEntitiesPFC

PFC found no evidence that personal information has been specifically misused; however, it is possible that the following information could have been accessed by an unauthorized third party: first and last name, address, accounts receivable balance and information regarding payments made to accounts, and, in some cases, date of birth, Social Security number, and health insurance and medical treatment information.

PFC is mailing letters to potentially involved individuals with details about the incident and providing resources they can use to help protect their information. PFC is also offering potentially involved individuals access to free credit monitoring and identity theft protection services through Cyberscout, a leading identity protection company.

Individuals should refer to the notice they received in the mail regarding steps they can take to protect themselves. As a precautionary measure, potentially impacted individuals should remain vigilant to protect against fraud and/or identity theft by, among other things, reviewing their financial account statements and monitoring free credit reports. If individuals detect any suspicious activity on an account, they should promptly notify the institution or company with which the account is maintained. Individuals should also promptly report any fraudulent activity or any suspected identity theft to proper law enforcement authorities, including the police and their state's attorney general.

> [. . .]
>
> Data security is one of PFC's highest priorities. Since the incident, PFC wiped and rebuilt affected systems and has taken steps to bolster its network security. PFC also reviewed and altered its policies, procedures, and network security software relating to the security of systems and servers, as well as how data is stored and managed.[27]

51. On or around July 1, 2022, Defendant began notifying Plaintiff and Class Members of the Data Breach.

52. On or about July 1, 2022, Defendant began reporting the breach to various states Attorneys General. For example, on or about July 1, 2022, Defendant reported to the Commonwealth of Massachusetts' Office of Consumer Affairs and Business Regulation that 4,224 Massachusetts residents were implicated in the Data Breach.[28] Next, on or around July 7, 2022, Defendant notified the Attorney General of Texas of the Data Breach.[29] Defendant reported to the Attorney General of Texas that, during the Data Breach, the attacker compromised the unprotected health information of more than 401,069 Texans.[30] In that report, Defendant confirmed that the affected information included "Name of individual; Address; Social Security Number Information; Medical Information; Health Insurance Information."[31]

53. On or about July 1, 2022, Defendant reported to the Department of Health and Human Services that the Data Breach impacted the unprotected health information of 1,918,941 individuals.

54. Defendant admitted in the sample breach notices that an unauthorized party accessed the PII and PHI of hundreds of thousands, if not millions, of individuals, including

[27] Ex. 1.
[28] https://www.mass.gov/doc/data-breach-report-2022/download (last visited July 7, 2022)
[29] https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited July 7, 2022).
[30] *Id.*
[31] *Id.*

Plaintiff and Class Members, including without limitation, first and last name, address, accounts receivable balance and information regarding payments made to accounts, and, in some cases, date of birth, Social Security number, and health insurance and medical treatment information.

55. In response to the Data Breach, Defendant claims that it "wiped and rebuilt affected systems and has taken steps to bolster its network security."[32] It also claims that it "reviewed and altered its policies, procedures, and network security software relating to the security of systems and servers, as well as how data is stored and managed."[33] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

56. Some or all of Plaintiff's and Class Members' PII and PHI that Defendant allowed to be compromised may find its way onto to the dark web, where it may be bought, sold and transferred in perpetuity, causing victims of the Data Breach untold harm. Alternatively, the wrongfully accessed, acquired, and/or misappropriated PII and PHI could simply fall into the hands of companies that will use the detailed PII and/or PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

57. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing their PII and PHI to be exposed.

58. Following the breach and recognizing that Plaintiff, along with each and every Class Member, is now subject to the present and continuing risk of identity theft and fraud,

[32] Ex. 1.

[33] Ex. 1.

Defendant offered Plaintiff and Class Members Single Credit Bureau Monitoring for twelve or twenty-four months through Cyberscout, a Transunion company. The offered services are insufficient to protect Plaintiff and Class Members from the lifelong implications of having their most private PII and PHI accessed and/or acquired by an unauthorized third party. As another element of damages, Plaintiff demands that Defendant provide a sum of money sufficient to provide to Plaintiff and Class Members identity theft protective services for their respective lifetimes as Plaintiff and Class Members as Plaintiff and Class Members are now and forever subject to an increased risk of identity theft due to the conduct of Defendant as described herein.

59. Further, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the offered services, among other steps Plaintiff and Class Members must take to protect themselves. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[34]

60. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[35] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[36] Usually, this time can be spent at the option and choice of the consumer,

[34] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, *available at* https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last visited July 7, 2022); *see also* U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data, available at* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last visited July 7, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[35] *See* James Wallman, *How Successful People Spend Leisure Time*, CNBC (Nov. 6, 2019), *available at* https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (last visited July 7, 2022).

[36] *Id.*

however, having been notified of the Data Breach, Plaintiff and Class Members now have to spend hours of their leisure time self-monitoring accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves and/or their children.

61. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

62. Plaintiff and Class Members now face years of constant surveillance of their financial, healthcare, and personal records. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

The Healthcare Sector is Particularly Susceptible to Data Breaches

63. Defendant was on notice that businesses in the healthcare industry are targets for data breaches. Much like other consumer facing businesses that collect and store large amounts of sensitive information, business affiliates of healthcare facilities have vast amounts of sensitive, valuable data, such as the PII and PHI at issue here.

64. However, the healthcare sector is a favored target by cybercriminals because, as demonstrated by recent studies, including one by the Massachusetts Institute of Technology, hospitals and their business associates lagged behind other businesses in safeguarding their computer systems.[37]

65. Indeed, a Tenable study analyzing healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of

[37] Jane Musgrave, *How two Palm Beach County Hospitals used paper to cope with a cyber attack,* PALM BEACH POST (Apr. 30, 2022), https://www.palmbeachpost.com/story/news/healthcare/2022/04/30/west-palm-beach-hospitals-handle-cyber-attack-ransomware-hive/9575400002/.

the breaches."[38] This case involves just such a breach of a computer system by an unknown third-party, and, accordingly, this Data Breach resulted in the unauthorized access, disclosure, and/or acquisition of the PII and PHI of Plaintiff and Class Members to unknown third-parties.

66. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[39]

67. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[40]

68. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[41] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[42] That trend

[38] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.
[39] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited July 7, 2022).
[40] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited July 7, 2022).
[41] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last visited July 7, 2022).
[42] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last visited July 7, 2022).

continues.

69. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[43] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[44] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[45]

70. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[46] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data

[43] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited July 7, 2022).
[44] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited July 7, 2022).
[45] *Id.*
[46] *2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/2019-himss-cybersecurity-survey (last visited July 7, 2022).

centers."[47]

71. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The compromised PII and PHI of Plaintiff and Class Members is in the hands of hackers who will misuse the information, including potentially offering the unencrypted, unredacted PII and PHI for sale on the dark web to other nefarious actors. Plaintiff and Class Members now face a present and continuing risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or acquisition by cybercriminals on computer systems containing millions of Social Security numbers and/or specific, sensitive medical information pertaining to healthcare services.

72. The Data Breach occurred due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members. Defendant still maintains as secret the specific vulnerabilities and root causes of the Data Breach. Plaintiff and Class Members also remain unaware of precisely what information was "accessed" and whether that information was copied and/or acquired by the cybercriminals, whether that information was recovered, and precisely how long the undetected cybercriminal(s) conducted unauthorized "activity" on Defendant's systems.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII and PHI.

73. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII and PHI.

74. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with this highly confidential PII and PHI.

[47] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited July 7, 2022).

75. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

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

Securing PII and Preventing Breaches

77. Defendant could have prevented this Data Breach by properly securing and encrypting the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially years-old data from former customers.

78. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

79. Despite the prevalence of public announcements of data breach and data security compromises Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

80. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[48] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

[48] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[49]

81. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

82. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[50] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[51] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[52]

83. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it

[49] *Id*.

[50] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited July 7, 2022).

[51] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited July 7, 2022).

[52] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited July 7, 2022).

> damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[53]

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

85. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The 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."[54]

86. Further, there is a market for Plaintiff's and Class Members PHI, and the stolen PII and PHI has inherent value. Sensitive healthcare data can sell for as much as $363 per record according to the Infosec Institute.[55]

87. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase

---

[53] SOCIAL SECURITY ADMINISTRATION, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 7, 2022).

[54] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 7, 2022).

[55] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), available at: https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited July 7, 2022).

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.

88. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[56]

89. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[57]

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

[56] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News (Feb. 7, 2014) available at: https://khn.org/news/rise-of-indentity-theft/ (last visited July 7, 2022).
[57] FBI Cyber Division, Private Industry Notification, "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," Apr. 8, 2014, *available at* http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited July 7, 2022).

91. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[58]

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

93. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

94. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[59]

Defendant's Conduct Violates HIPAA

95. 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 has subsequently promulgated five

[58] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 7, 2022).

[59] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last visited July 7, 2022).

rules under authority of the Administrative Simplification provisions of HIPAA.

96. Defendant's Data Breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff and Class Members' PII and PHI.

97. In addition, Defendant's Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PII and PHI when it was no longer necessary and/or had honored its obligations to its customers.

98. Defendant's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

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

f. Failing 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 CFR 164.308(a)(6)(ii);

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

h. Failing 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 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*; and

k. Retaining information past a recognized purpose and not deleting it.

99. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[60]

100. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate.

101. Defendant still maintains the protected health information and other PII of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' protected health information and other PII remains at risk of subsequent Data

[60] Breach Notification Rule, U.S. DEP'T OF HEALTH & HUMAN SERVICES, *available at*: hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Oct. 13, 2020).

Breaches.

Defendant Failed to Comply with FTC Guidelines

102. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

103. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that 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.[61]

104. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[62] The guidelines note that businesses should protect the personal customer 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.

105. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords

[61] FEDERAL TRADE COMMISSION, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 7, 2022).
[62] FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 7, 2022).

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.[63]

106. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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.

107. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

108. Defendant was at all times fully aware of its obligation to protect the PII stored within its systems because of its position as a leading healthcare business affiliate. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Plaintiff and Class Members Suffered Damages

109. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

110. Plaintiff and Class Members now face years of constant surveillance of their

[63] FTC, *Start With Security*, *supra*.

financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

111. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system, amounting to millions of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

112. Following the breach and recognizing that Plaintiff, along with each and every Class Member, is now subject to the present and continuing risk of identity theft and fraud, Defendant offered Plaintiff and Class Members Single Bureau Credit Monitoring for twelve months through a single credit bureau – Transunion. The offered services are insufficient to protect Plaintiff and Class Members from the lifelong implications of having their most private PII and PHI accessed, acquired, exfiltrated, and/or published onto the internet.

113. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Natalie Willingham's Experience

114. Plaintiff was a patient of one of Defendant's customers, Touchstone Medical Imaging in late 2019 or early 2020. As a condition of that care, Plaintiff was required to provide her personal and medical information, including her Social Security number.

115. Plaintiff entrusted her PII and PHI to Defendant.

116. Prior to the Data Breach, Defendant retained Plaintiff's first and last name, address, accounts receivable balance and information regarding payments made to her account, and Social Security number along with her PHI within Defendant's systems.

117. On or about July 5, 2022, Plaintiff received a Notice of Data Breach from Defendant, dated July 1, 2022 that informed her of the Data Breach and that her information was impacted or "involved." This was the first communication Plaintiff had ever received from Defendant and first time she learned that Defendant had access to her information.

118. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through her unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, attempting to enroll in the credit monitoring and identity theft protection services offered by Defendant, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

119. Additionally, Plaintiff is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff stores any documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

120. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Plaintiff entrusted to Defendant through Touchstone Medical Imaging for the purpose of obtaining healthcare, which was compromised in and as a result of the Data Breach.

121. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy. Plaintiff has also experienced a significant uptick in spam text messages, calls, mail, and emails since the Data Breach.

122. Plaintiff has suffered further injury arising from the present and continuing risk of fraud, identity theft, and misuse resulting from her PII and PHI being accessed by and/or placed in the hands of unauthorized third parties and cybercriminals.

123. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

124. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, and other applicable law.

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

> All United States residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Cybersecurity Incident that Defendant published to Plaintiff and other Class Members on or around July 1, 2022 **(the "Nationwide Class")**.

126. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff members.

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

128. This action is brought and may be maintained as a class action because there is a

well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiff and Class Members were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

129. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**: The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least one million Class Members. Those individuals' names and addresses are available from Defendant's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

130. **Commonality: Fed. R. Civ. P. 23(a)(2) and (b)(3)**: Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

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

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and

Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

h. 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;

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

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

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

131. **Typicality: Fed. R. Civ. P. 23(a)(3):** Consistent with Rule 23(a)(3), Plaintiff is a member of the Class she seeks to represent and her claims and injuries are typical of the claims and injuries of the other Class Members. Plaintiff's PII and PHI was in Defendant's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class Members and Plaintiff seek relief consistent with the relief of the Class.

132. **Adequacy: Fed. R. Civ. P. 23(a)(4):** Consistent with Rule 23(a)(4), Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests

adverse to the interests of absent Class Members. Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests

133. **Predominance & Superiority: Fed. R. Civ. P. 23(b)(3):** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

134. **Injunctive and Declaratory Relief**. Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate

respecting the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

135. Likewise, particular issues under Rule 23(c)(4) 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 owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their PII and PHI;

b. Whether Defendant failed to take commercially reasonable steps to safeguard the PII and PHI of Plaintiff and the Class Members;

c. Whether Defendant failed to adequately monitor and audit its data security systems that stored PII and PHI;

d. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

136. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such

individuals to effectively pursue recovery of the sums owed to them.

137. **Risk of Prosecuting Separate Actions:** This case is appropriate for certification because class action litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

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

138. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 137.

139. Plaintiff and the Nationwide Class provided and entrusted Defendant and/or the Covered Entities with certain PII and PHI, including, without limitation, first and last name, address, accounts receivable balance and information regarding payments made to accounts, and, in some cases, date of birth, Social Security number, and health insurance and medical treatment information.

140. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

141. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII and PHI were wrongfully disclosed.

142. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm

occurred through the criminal acts of a third party.

143. Defendant 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. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

144. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and PHI it was no longer required to retain pursuant to contractual obligations or state and federal regulations, including that of former customers or patients.

145. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Nationwide Class.

146. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential PII and PHI, a necessary part of their relationships with Defendant.

147. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Nationwide Class.

148. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

149. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and Class Members, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting

PII and PHI stored on Defendant's systems.

150. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and Class Members, including basic encryption techniques freely available to Defendant.

151. Plaintiff and the Nationwide Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

152. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

153. Defendant had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

154. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and Class Members.

155. Defendant has admitted that the PII and PHI of Plaintiff and the Nationwide Class was wrongfully accessed by, disclosed to, and/or acquired by unauthorized third persons as a result of the Data Breach.

156. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise

reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide Class during the time the PII and PHI was within Defendant's possession or control.

157. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

158. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Nationwide Class in the face of increased risk of theft.

159. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII and PHI.

160. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII and PHI it was no longer required to retain pursuant to regulations.

161. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

162. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII and PHI of Plaintiff and the Nationwide Class would not have been compromised.

163. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII and PHI of Plaintiff and the Nationwide Class was compromised as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and

maintaining appropriate security measures.

164. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

165. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

166. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

167. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

168. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

169. Defendant's violation of HIPAA also independently constitutes negligence *per se*.

170. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present

a risk of harm to the patient's finances or reputation.

171. Plaintiff and the Nationwide Class are within the class of persons that HIPAA privacy laws were intended to protect.

172. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

173. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

174. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

175. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

176. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

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

177. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 137.

178. Defendant required Plaintiff and the Nationwide Class to provide and entrust their PII and PHI, including, without limitation, first and last name, address, accounts receivable balance and information regarding payments made to accounts, and, in some cases, date of birth, Social Security number, and health insurance and medical treatment information.

179. Defendant solicited and invited Plaintiff and the Nationwide Class to provide their PII and PHI to Defendant, either directly or indirectly through Defendant's customers, the Covered Entities, as part of Defendant's regular business practices. Plaintiff and the Nationwide Class accepted Defendant's offers and provided their PII and PHI to Defendant.

180. As a condition of obtaining care and/or services from Defendant, Plaintiff and the Nationwide Class provided and entrusted their personal information. In so doing, Plaintiff the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to

timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

181. A meeting of the minds occurred when Plaintiff and the Nationwide Class agreed to, and did, provide their PII and PHI to Defendant and/or Defendant's customers, in exchange for, amongst other things, the protection of their PII and PHI.

182. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

183. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by failing to comply with its promise to abide by HIPAA.

184. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

185. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

186. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

187. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by failing 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 CFR 164.308(a)(6)(ii).

188. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

189. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by failing 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 CFR 164.306(a)(3).

190. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

191. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

192. Defendant further breached the implied contracts with Plaintiff and the Nationwide Class by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

193. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the Data Breach.

194. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary

loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

195. As a result of Defendant's breach of implied contract, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and Class Members)

196. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 134.

197. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

198. Defendant owed a duty to its customers and their patients, including Plaintiff and Class Members, to keep the PII and PHI entrusted to it and contained in its systems confidential.

199. Defendant failed to protect and allowed access to and/or released to unknown and unauthorized third parties the PII and PHI of Plaintiff and Class Members.

200. Defendant allowed unauthorized and unknown third parties to access and examine of the PII and PHI of Plaintiff and Class Members, by way of Defendant's failure to protect the PII and PHI.

201. The unauthorized release to, custody of, and/or examination by unauthorized third parties of the PII and PHI of Plaintiff and the Nationwide Class is highly offensive to a reasonable

person.

202. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII and PHI to Defendant as part of Plaintiff's and Class Members' relationships with Defendant, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

203. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

204. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

205. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

206. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

207. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no

adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and Class Members)

208. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 137.

209. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII and PHI that Plaintiff and the Nationwide Class provided to Defendant and/or Defendant's customers.

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

211. Plaintiff and the Nationwide Class provided their PII and PHI to Defendant and/or Defendant's customers with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

212. Plaintiff and the Nationwide Class also provided their PII and PHI to Defendant, either directly or indirectly, with the explicit and implicit understandings that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

213. Defendant voluntarily received in confidence the PII and PHI of Plaintiff and the Nationwide Class with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

214. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII and PHI of Plaintiff and the Nationwide Class was disclosed and/or misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

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

216. But for Defendant's disclosure of Plaintiff's and Class Members' PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised by unauthorized third parties. The Data Breach was the direct and legal cause of access, disclosure, acquisition, and/or theft of Plaintiff's and Class Members' PII and PHI as well as the resulting damages.

217. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and Class Members' PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' PII and PHI.

218. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and Class Members, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, 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 PII and PHI of Plaintiff and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

219. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

220. As a result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT V
Violation of Colorado Consumer Protection Act,
Colo. Rev. Stat. § 6-1-101, *et seq.*
(On behalf of Plaintiff and the Nationwide Class)

221. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 137.

222. The Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-105(1)(l), *et seq*., prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service.

223. Defendant is a "person" under § 6-1-102(6) of the Colorado Consumer Protection Act ("Colorado CPA"), Colo. Rev. Stat. § 6-1-101, *et seq*.

224. Plaintiff and the Nationwide Class are current and former patients of Defendant's customers who, for the purposes of receiving healthcare services and subsequently

paying Defendant for any accounts due, provided sensitive and confidential PII and PHI to Defendant, which PFC collected, stored, and maintained at its Colorado headquarters.

225. Defendant is engaged in, and its acts and omissions affect, trade and commerce.

226. Defendant's relevant acts, practices and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services throughout the United States.

227. In the conduct of its business, trade, and commerce, and in the sale of debt collection services to and/or from consumers, Defendant engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of services to consumers. Plaintiff and other members of the Nationwide Class furnished or purchased these services. Plaintiff and the Nationwide Class are actual or potential consumers as defined by Colo. Rev. Stat § 6-1-113(1), *et seq.*

228. In the conduct of its business, trade, and commerce, and in the sale of debt collection services to and/or from consumers, Defendant collected and stored highly personal and private information, including PII and PHI belonging to Plaintiff and the Nationwide Class.

229. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII and PHI of Plaintiff and the Nationwide Class and that the risk of a data breach was highly likely and/or that the risk of the Data Breach being more extensive than originally disclosed was highly likely.

230. Defendant should have disclosed this information regarding its computer systems and data security practices because Defendant was in a superior position to know the true facts related to the defect, and Plaintiff and the Nationwide Class could not reasonably be expected to learn or discover the true facts.

231. As alleged herein this Complaint, Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the furnishing of debt collection services to and/or from consumers in violation of the Colorado Consumer Protection Act, including but not limited to the following:

a. failing to adequately secure customer names and Social Security numbers;

b. failing to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information;

c. failing to disclose the material information, known at the time of the transaction – collection and retention of the customers' PII and PHI to furnish debt collection services – that its computer systems would not adequately protect and safeguard the PII and PHI it collected and maintained;

d. inducing consumers to use Defendant's services by failing to disclose, and misrepresenting the material fact that Defendant's computer systems and data security practices were inadequate to safeguard sensitive personal information from unauthorized access and/or theft.

232. By engaging in the conduct delineated above, Defendant has violated the Colorado Consumer Protection Act by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the security of the transactions between Defendant and its customers;

c. omitting material facts regarding the security of the transactions between Defendant and its customers for whom it furnished debt collection services;

d. misrepresenting material facts in the furnishing or sale of products, goods or services to consumers;

e. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

f. engaging in conduct which creates a likelihood of confusion or of misunderstanding;

g. engaging in conduct with the intent to induce consumers to use Defendant's service;

h. unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

i. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

233. Defendant systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiff and the Nationwide Class.

234. Defendant's actions in engaging in the conduct delineated above were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Nationwide Class.

235. As a direct result of Defendant's violation of the Colorado Consumer Protection Act, Plaintiff and the Nationwide Class have suffered actual damages, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover

from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, 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 that PII and PHI; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

236. As a result of Defendant's violation of the Colorado Consumer Protection Action, Plaintiff and the Nationwide Class are entitled to, and seek, injunctive relief, including, but not limited to:

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

b. Ordering that Defendant engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding new or modified procedures;

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

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner employee and customer data not necessary for its provision of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Defendant to meaningfully educate its employees and customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

237. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Defendant alleged herein, Plaintiff and the Nationwide Class seek relief under Colo. Rev. Stat. § 6-1-113, including, but not limited to, the greater of actual damages, statutory damages, or treble damages for bad faith conduct, injunctive relief, attorneys' fees and costs, as allowable by law.

PRAYER FOR RELIEF

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

A. For an Order certifying the Nationwide Class and appointing Plaintiff and their Counsel to represent such 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 PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

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

Class Members, including but not limited to an order:

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

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

v. prohibiting Defendant from maintaining the PII and PHI of Plaintiff and the Nationwide Class 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 Plaintiff 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 the Nationwide Class 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, consequential, nominal, and statutory 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.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: July 14, 2022

Respectfully Submitted,

/s/ *Kevin Hannon*

Kevin Hannon, Esq.
CO Bar No. 16015
THE HANNON LAW FIRM, LLC
1641 Downing Street
Denver, CO 80128
303-861-8800

khannon@hannonlaw.com

JEAN S. MARTIN
(*Pro Hac Vice application forthcoming*)
FRANCESCA KESTER
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

Attorneys for Plaintiff and the Putative Class