

IN THE IOWA DISTRICT COURT FOR LINN COUNTY

---

BRANDI BELL individually, and BRANDIE KEEGAN, individually and on behalf of her minor child, E.S., and on behalf of all others similarly situated,	Case No. CVCV104303
Plaintiffs,	AMENDED PETITION AT LAW
v.	JURY TRIAL DEMANDED
C.R. PHARMACY SERVICES, INC. d/b/a CAREPRO HEALTH SERVICES,	
Defendant.	

---

Plaintiffs Brandi Bell and Brandie Keegan (“Plaintiffs”) bring this Class Action Complaint (“Complaint”) against Defendant C.R. Pharmacy Services, Inc. d/b/a CarePro Health Services (“CarePro” or “Defendant”), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels’ investigation, and upon information and belief as to all other matters, as follows:

**NATURE OF THE ACTION**

1. This class action arises out of the recent cyberattack and data breach (“Data Breach”) resulting from CarePro's failure to implement reasonable and industry standard data security practices.

2. Defendant is an Iowa-based company that “offers a wide variety of medical services” to its patients.<sup>1</sup>

---

<sup>1</sup> <https://www.careprohs.com/>

3. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

4. CarePro collected and maintained certain personally identifiable information of Plaintiffs and the putative Class Members (defined below), who are (or were) patients at CarePro.

5. The Private Information compromised in the Data Breach included Plaintiffs' and Class Members' full names, contact information, dates of birth, state IDs, Social Security numbers, driver's license numbers, and financial account information. (“personally identifiable information” or “PII”) and medical and health insurance information, which is protected health information (“PHI”, and collectively with PII, “Private Information”) as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

6. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

7. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) Plaintiffs' Private Information being disseminated on the dark web, according to Experian (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains

backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' Private Information from a foreseeable and preventable cyber-attack.

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

10. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

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

12. Armed with the Private Information accessed in the Data Breach, data thieves have

already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

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

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

15. Plaintiffs bring this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

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

17. Plaintiffs seek remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

**PARTIES**

18. Plaintiff, Brandi Bell, is a natural person and citizen of Iowa City, Iowa.

19. Plaintiff Brandie Keegan is a natural person and citizen of Iowa, residing in Davenport, Iowa. Her daughter, a minor, is a former patient of CarePro. Ms. Keegan and/or her daughter's Personal Information was compromised by the Data Breach.

20. Defendant, C.R. Pharmacy Services, Inc. d/b/a CarePro Health Services, is a corporation organized under the state laws of Iowa, with its principal place of business located in Cedar Rapids, Iowa.

**JURISDICTION AND VENUE**

21. This Court has personal jurisdiction over CarePro because Defendant regularly solicits business in the state of Iowa and committed the tortious acts complained of in the state of Iowa. This case arises entirely out of transactions conducted within the state. Defendant markets and/or sells its products and services in the state of Iowa and is responsible for the advertising and/or marketing of its medical products and services.

22. Venue is proper in this District because Defendant's principal place of business is located in the District and Defendant conducts a substantial amount of business in this District.

**FACTUAL ALLEGATIONS**

***Background***

23. Defendant is an Iowa-based company that "offers a wide variety of medical services" to its patients.<sup>2</sup>

24. Plaintiffs and Class Members are current and former patients at Defendant.

25. Upon information and belief, in the course of collecting Private Information from

---

<sup>2</sup> <https://www.careprohs.com/>

patients, including Plaintiffs, Defendant promised to provide confidentiality and adequate security for patient data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

26. Indeed, Defendant provides on its website that: “CarePro Health Services is required by law to maintain the privacy of Protected Health Information[.]”<sup>3</sup>

27. In the course of their relationship, patients, including Plaintiffs and Class Members, provided Defendant with at least the following: names, contact information, dates of birth, health insurance information, Social Security numbers, and other sensitive information.

28. Plaintiffs and Class Members, as former and current patients of Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when PHI and other sensitive Private Information is involved.

### ***The Data Breach***

29. In the untitled letters (the “Notice Letter”) sent to Plaintiffs and Class Members, dated on or about January 23, 2024, Defendant asserts that:

**What Happened?** On or around November 16, 2023, CarePro experienced a network disruption incident which affected our ability to access certain systems. We immediately took steps to secure our network and began an investigation, which included working with third-party specialists to assist in our investigation to determine the nature and scope of the activity. Our investigation revealed that certain information within our systems was acquired by an unauthorized individual on or around November 14, 2023. We immediately began a review of our systems to determine the types of information that were potentially at risk. As part of this review, we initiated efforts to obtain up-to-date address information for all potentially affected individuals. On January 11, 2024, this process was completed, and we worked to provide you with this notification as soon as

---

<sup>3</sup> <https://www.careprohs.com/privacy-policy>

possible.

**What Information Was Involved?** The information potentially at risk during the incident may have included your first and last name in combination with the following data element(s): contact information, date of birth, diagnosis/condition information, treatment information, treatment cost information, lab results, service date, provider name, prescription information, health insurance and/or claim information, Social Security number, driver's license number or financial account information.<sup>4</sup>

30. Omitted from the Notice Letter were the details of root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

31. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a healthcare entity that collects, creates, and maintains Private Information on its computer networks and/or systems.

32. As Defendant's Notice Letter admits, Plaintiffs' and Class Members' Private Information was, in fact, compromised and acquired in the Data Breach.

33. The files containing Plaintiff's and Class Members' Private Information, that were targeted and stolen from Defendant, included their names, Social Security numbers, PHI, and other sensitive information.

34. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiffs and Class Members.

---

<sup>4</sup> The "Notice Letter". A sample copy is available at <https://ago.vermont.gov/sites/ago/files/documents/2024-01-23%20CR%20Pharmacy%20Services%20dba%20CarePro%20Services%20Data%20Breach%20Notice%20to%20Consumers.pdf>

35. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

36. Plaintiff Bell has been informed by Experian that her Private Information has already been disseminated on the dark web, and Plaintiffs further believe that the Private Information of Class Members was accessed and stolen in the Data Breach and is currently or will become available for sale on the dark web because that is the *modus operandi* of cybercriminals.

37. Defendant had obligations created by the FTC Act, HIPAA, contract, state and federal law, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

***Data Breaches Are Preventable***

38. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

39. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

40. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, patients and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.<sup>5</sup>

41. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

**Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

---

<sup>5</sup> *Id.* at 3-4.

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].<sup>6</sup>

42. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

43. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of approximately 151,000 patients' Private Information,<sup>7</sup> including that of Plaintiffs and Class Members.

***Defendant Acquires, Collects, And Stores Patients' Private Information***

44. Defendant acquires, collects, and stores a massive amount of Private Information on its patients, former patients and other personnel.

45. As a condition of obtaining medical services from CarePro, Defendant requires that patients entrust it with highly sensitive personal information.

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

47. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

---

<sup>6</sup> See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

<sup>7</sup> [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

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

***Defendant Knew or Should Have Known of the Risk Because Pharmaceutical Companies In Possession Of Private Information Are Particularly Susceptable To Cyber Attacks***

49. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting pharmaceutical companies that collect and store Private Information, like Defendant, preceding the date of the breach.

50. Data breaches, including those perpetrated against pharmaceutical companies that store Private Information in their systems, have become widespread.

51. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801).<sup>8</sup> The ITRC set a new record for the number of data compromises tracked in a year, up 72 percentage points from the previous all-time high in 2021 (1,860).<sup>9</sup>

52. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have

---

<sup>8</sup> <https://www.idtheftcenter.org/publication/2023-data-breach-report/>

<sup>9</sup> *Id.*

known that its electronic records would be targeted by cybercriminals.

53. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>10</sup>

54. Defendant knew and understood unprotected or exposed Private Information in the custody of pharmaceutical companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

55. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

57. The injuries to Plaintiffs and Class Members were directly and proximately caused

---

<sup>10</sup> [https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl\\_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=consumerprotection](https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection)

by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

58. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

59. As a pharmaceutical company in custody of current and former patients' Private Information, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

***Value Of Personally Identifiable Information***

60. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."<sup>11</sup> The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."<sup>12</sup>

61. The Private Information of individuals remains of high value to criminals, as

---

<sup>11</sup> 17 C.F.R. § 248.201 (2013).

<sup>12</sup> *Id.*

evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.<sup>13</sup>

62. For example, PII can be sold at a price ranging from \$40 to \$200.<sup>14</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>15</sup>

63. PII can sell for as much as \$363 per record according to the Infosec Institute.<sup>16</sup> PII is particularly valuable because criminals can use it to target victims with frauds and scams.

64. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

65. Social Security numbers, which were compromised for some of the Class Members as alleged herein, for example, are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as 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 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.<sup>17</sup>

---

<sup>13</sup> *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/>

<sup>14</sup> *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/>

<sup>15</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (

<sup>16</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

<sup>17</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

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

67. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link 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."<sup>18</sup>

68. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."<sup>19</sup>

69. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200."<sup>20</sup>

70. According to national credit bureau Experian:

A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number

---

<sup>18</sup> 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>

<sup>19</sup> *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, available at: <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658> .

<sup>20</sup> <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658>

can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

71. According to cybersecurity specialty publication CPO Magazine, “[t]o those unfamiliar with the world of fraud, driver’s license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation.”<sup>21</sup> However, this is not the case. As cybersecurity experts point out:

“It’s a gold mine for hackers. With a driver’s license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.”<sup>22</sup>

72. Victims of driver’s license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.<sup>23</sup>

73. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”<sup>24</sup>

74. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.*, patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient’s complete record can be sold for hundreds of dollars on the dark

---

<sup>21</sup> <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/>

<sup>22</sup> *Id.*

<sup>23</sup> *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021, available at: <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html>

<sup>24</sup> *Medical I.D. Theft, EFraudPrevention*  
<https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected>

web. As such, PHI/PII is a valuable commodity for which a “cyber black market” exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

75. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.<sup>25</sup> Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.<sup>26</sup> In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.<sup>27</sup>

76. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.<sup>28</sup>

77. “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.”<sup>29</sup>

78. A study by Experian found that the average cost of medical identity theft is “about \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-

---

<sup>25</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/>

<sup>26</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/>

<sup>27</sup> <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/>

<sup>28</sup> Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>

<sup>29</sup> Brandi Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>

pocket costs for healthcare they did not receive to restore coverage.<sup>30</sup> Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.<sup>31</sup>

79. 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—names, Social Security numbers, and PHI.

80. 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 . . . [is] worth more than 10x on the black market.”<sup>32</sup>

81. 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.

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

---

<sup>30</sup> See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar, 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>

<sup>31</sup> *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>

<sup>32</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

[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.<sup>33</sup>

***Defendant Fails To Comply With FTC Guidelines***

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

84. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.<sup>34</sup>

85. The guidelines also recommend that healthcare businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>35</sup>

86. The FTC further recommends that healthcare companies not maintain Private

---

<sup>33</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

<sup>34</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)

<sup>35</sup> *Id.*

Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

87. The FTC has brought enforcement actions against healthcare entities for failing to protect patient data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient 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.

88. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (CarePro) ¶ 79708, 2016 WL 4128215, at \*32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

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

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

91. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

***Defendant Fails To Comply With HIPAA Guidelines***

92. Defendant is a business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

93. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).<sup>36</sup> See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

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

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

98. HIPAA’s Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic

---

<sup>36</sup> HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

protected health information the covered entity or business associate creates, receives, maintains, or transmits;

- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

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

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

101. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”<sup>37</sup>

---

<sup>37</sup> Breach Notification Rule, U.S. Dep’t of Health & Human Services,

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

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

104. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material.<sup>38</sup> The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.<sup>39</sup>

***Defendant Fails To Comply With Industry Standards***

---

<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

<sup>38</sup> <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

<sup>39</sup> <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

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

106. Several best practices have been identified that, at a minimum, should be implemented by pharmaceutical companies in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

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

108. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

109. These foregoing frameworks are existing and applicable industry standards in the

pharmaceutical industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

**COMMON INJURIES & DAMAGES**

110. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

***The Data Breach Increases Victims' Risk Of Identity Theft***

111. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

112. As Plaintiff Bell has already experienced, the unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

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

114. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

115. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

116. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.<sup>40</sup>

---

<sup>40</sup> "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule

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

118. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

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

120. Thus, even if certain information (such as Social Security numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

121. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

***Loss Of Time To Mitigate Risk Of Identity Theft And Fraud***

---

account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

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

123. Thus, due to the actual and imminent risk of identity theft, Defendant in its Notice Letter, instructs Plaintiffs and Class Members to take the following measures to protect themselves: “[w]e recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors.”<sup>41</sup>

124. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, upon receiving the Notice Letter, changing their phone numbers, contacting credit bureaus to place freezes on their accounts, contacting the Federal Trade Commission, Contracting the Internal Revenue Service, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

125. Plaintiffs’ mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their

---

<sup>41</sup> Notice Letter.

good name and credit record.”<sup>42</sup>

126. Plaintiffs’ mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>43</sup>

127. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>44</sup>

### ***Diminution Value Of Private Information***

128. PII and PHI are valuable property rights.<sup>45</sup> Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

---

<sup>42</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

<sup>43</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

<sup>44</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

<sup>45</sup> See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

129. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>46</sup>

130. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.<sup>47,48</sup>

131. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>49</sup>

132. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.<sup>50</sup>

133. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”<sup>51</sup>

134. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.<sup>52</sup>

135. As a result of the Data Breach, Plaintiffs’ and Class Members’ Private Information,

---

<sup>46</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

<sup>47</sup> <https://datacoup.com/>

<sup>48</sup> <https://digi.me/what-is-digime/>

<sup>49</sup> Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html>

<sup>50</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

<sup>51</sup> *Medical I.D. Theft, EFraudPrevention* <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.>

<sup>52</sup> Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>

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

136. 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, e.g., names, Social Security numbers, dates of birth, and PHI.

137. 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.

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

139. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

140. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s network, amounting to more than one hundred thousand individuals’ detailed personal information, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

141. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

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

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

143. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her personal information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

144. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

145. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but

for Defendant's failure to safeguard their Private Information.

***Loss Of The Benefit Of The Bargain***

146. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for the provision of pharmaceutical services, Plaintiffs and other reasonable patients understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received pharmaceutical services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

**PLAINTIFF BELL'S EXPERIENCE**

147. Plaintiff Brandi Bell is a current patient at Defendant.

148. In order to obtain pharmaceutical services at Defendant, she was required to provide her Private Information to Defendant.

149. At the time of the Data Breach—on or around November 14, 2023—Defendant retained Plaintiff's Private Information in its system.

150. Plaintiff Bell is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

151. Plaintiff Bell received the Notice Letter, by U.S. mail, directly from Defendant, dated January 23, 2024. According to the Notice Letter, Plaintiff's PII and PHI was improperly accessed and obtained by unauthorized third parties, including her name, contact information,

date of birth, diagnosis/condition information, treatment information, treatment cost information, lab results, service date, provider name, prescription information, health insurance and/or claim information, Social Security number, driver's license number, and financial account information.

152. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff to "remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors[,]”<sup>53</sup> Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, upon receiving the Notice Letter, changing her phone number, contacting credit bureaus to place freezes on her accounts, contacting the Federal Trade Commission, Contracting the Internal Revenue Service, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

153. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which:

---

<sup>53</sup> Notice Letter.

(a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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 Private Information.

154. Plaintiff further suffered actual injury in the form of her Private Information being disseminated on the dark web, according to Experian, which, upon information and belief, was caused by the Data Breach.

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

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

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

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

#### **PLAINTIFF KEEGAN'S EXPERIENCE**

159. Plaintiff Brandie Keegan's minor daughter is a former patient of CarePro.

160. As a condition of providing health services, CarePro required Ms. Keegan and her daughter to provide their PII and PHI.

161. Ms. Keegan provided CarePro with her daughter's PII and PHI as a condition of receiving health services from CarePro. Ms. Keegan would not have provided her daughter's PII

and PHI to CarePro had she known that CarePro would not protect it as promised.

162. On or after January 23, 2024, Ms. Keegan received a notice from CarePro and became aware that her and/or her daughter's Personal Information was impacted by the Data Breach.

163. Ms. Keegan attempted to enroll her daughter in the free credit monitoring program provided by CarePro but was unable to enroll E.S., given E.S.'s status as a minor.

164. As a further result of the Data Breach, Ms. Keegan expends considerable time and effort monitoring her accounts to protect herself and E.S. from additional identity theft. Ms. Keegan fears for hers and E.S.'s personal financial security and is experiencing feelings of rage and anger, anxiety, sleep disruption, stress, fear, and physical pain. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

165. Ms. Keegan and E.S. remain at a continued risk of harm due to the exposure and potential misuse of their personal data by criminal hackers.

### **CLASS ACTION ALLEGATIONS**

166. Pursuant to Iowa R. Civ. P. 1.261; 1.262 and 1.263, Plaintiffs bring this action on behalf of themselves and all other persons similarly situated.

167. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

#### **Nationwide Class**

All persons whose Private Information was compromised as a result of the Data Breach, for which Defendant provided notice in January 2024 (the "Class").

168. Excluded from the Class are Defendant's officers and directors, and any entity in

which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

169. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification.

170. Numerosity – Iowa R. Civ. P. 1.262(1). The Members of the Class are so numerous that joinder of all of them is impracticable. Although the precise number of individuals impacted in the Data Breach is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, more than 151,000 persons were impacted in the Data Breach.<sup>54</sup>

171. Commonality - Iowa R. Civ. P. 1.262(2). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach

---

<sup>54</sup> [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

were consistent with industry standards;

- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breached implied contracts for adequate data security with Plaintiffs and Class Members;
- l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiffs and Class Members;
- m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,
- n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

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

173. Adequacy of Representation - Iowa R. Civ. P. 1.263(2). Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

174. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

175. Superiority Iowa R. Civ. P. 1.262(2). A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

176. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

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

- a. Whether Defendant failed to timely notify the public of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard patients' Private Information; and
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

**COUNT I**  
**Negligence**  
**(On Behalf of Plaintiffs and the Class)**

179. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

180. Defendant requires its patients, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its pharmaceutical services.

181. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

182. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

183. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

184. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

186. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or

disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

187. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiffs or Class Members of the Data Breach until January 23, 2024 despite, upon information and belief, Defendant knowing shortly after November 16, 2023 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

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

189. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of being patients of Defendant.

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

191. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

192. Defendant also had a duty to exercise appropriate clearinghouse practices to remove

former patients' Private Information it was no longer required to retain pursuant to regulations.

193. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

194. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the 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 Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

195. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- f. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations,

- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

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

197. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

198. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

199. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

200. 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 Plaintiffs and the Class.

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

202. It was foreseeable that Defendant's failure to use reasonable measures to protect

Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the pharmaceutical industry.

203. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

204. Plaintiffs and the 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 Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

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

206. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

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

208. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

209. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

210. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

211. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

212. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) Plaintiff Bell's Private Information being disseminated on the dark web, according to Experian (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

213. As a direct and proximate result of Defendant's negligence, Plaintiffs and the 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.

214. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

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

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

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

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

218. Plaintiffs re-allege and incorporate each of the foregoing paragraphs as if fully set forth herein.

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

220. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

221. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiffs or Class Members of the Data Breach until January 23, 2024 despite, upon information and belief, Defendant knowing shortly after November 16, 2023 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

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

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

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

225. The harm resulting from the Data Breach was the harm the FTC Act and HIPAA were intended to guard against and Plaintiffs and Class Members are within the class of persons the statutes were intended to protect.

226. The injury and harm suffered by Plaintiffs and Class Members was the reasonably

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

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

**COUNT III**  
**Breach Of Implied Contract**  
**(On Behalf of Plaintiff and the Class)**

228. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

229. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of receiving pharmaceutical services from Defendant.

230. Plaintiffs and the Class entrusted their Private Information to Defendant. In so doing, Plaintiffs and the 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 Plaintiffs and the Class if their data had been breached and compromised or stolen.

231. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of

their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

232. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

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

234. In accepting the Private Information of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

235. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

236. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

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

238. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security.

Defendant failed to do so.

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

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

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

242. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

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

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

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

**COUNT IV**  
**Invasion of Privacy**

**(On Behalf of Plaintiff and the Class)**

246. Plaintiffs re-allege and incorporate each of the foregoing paragraphs as if fully set forth herein.

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

248. Defendant invaded Plaintiffs' and the Class Members' right to privacy by allowing the unauthorized access to Plaintiffs' and Class Members' Private Information and by negligently maintaining the confidentiality of Plaintiffs' and Class Members' Private Information, as set forth above.

249. The intrusion was offensive and objectionable to Plaintiffs, the Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiffs' and Class Members' Private Information was disclosed without prior written authorization of Plaintiffs and the Class.

250. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs and the Class Members provided and disclosed their Private Information to Defendant privately with an intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

251. As a direct and proximate result of Defendant's above acts, Plaintiffs' and the Class Members' Private Information was viewed, distributed, and used by persons without prior written authorization and Plaintiffs and the Class Members suffered damages as described herein.

252. Defendant has committed oppression, fraud, or malice by permitting the

unauthorized disclosure of Plaintiffs' and the Class Members' Private Information with a willful and conscious disregard of Plaintiffs' and the Class Members' right to privacy.

253. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs and the Class, and Defendant may freely treat Plaintiffs' and Class Members' Private Information with sub-standard and insufficient protections.

254. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiffs and the Class Members great and irreparable injury in that the Private Information maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons.

**COUNT V**  
**Breach of Fiduciary Duty**  
**(On Behalf of Plaintiffs and the Class)**

255. Plaintiffs re-allege and incorporate each of the foregoing paragraphs as if fully set forth herein.

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

257. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep

secure their Private Information.

258. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members because of the high degree of trust and confidence inherent to the nature of the relationship between Plaintiffs and Class Members on the one hand and Defendant on the other, including with respect to their Private Information.

259. Plaintiffs and Class Members were entirely reliant on Defendant to use its expertise and knowledge to implement appropriate and reasonable measures to protect their Private Information. Plaintiffs and Class Members had no way to influence Defendant's data security practices or to verify their integrity.

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

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

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

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

Plaintiff Bell's Private Information being disseminated on the dark web, according to Experian (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

**COUNT VI**  
**Breach of Confidence**  
**(On Behalf of Plaintiffs and the Class)**

265. Plaintiffs re-allege and incorporate each of the foregoing paragraphs as if fully set forth herein.

266. At all times during Plaintiffs' and Class Members' interactions with Defendant and/or its agents, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Personal Information.

267. Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized parties.

268. Plaintiffs and Class Members provided their Private Information to Defendant and/or its agents with the explicit and implicit understanding that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

269. Plaintiffs and Class Members also provided their Private Information to

Defendant and/or its agents with the explicit and implicit understandings that Defendant would take precautions to protect such Private Information from unauthorized disclosure.

270. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

271. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

272. As a direct and proximate result of Defendant's acts and/or omissions, Plaintiffs and Class Members have suffered damages.

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

274. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information.

275. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class Members have suffered and will suffer injury and damages as set forth herein,

including monetary damages, fraudulent misuse of their Private Information and fraudulent charges; loss of the opportunity to control how their Private Information is used; diminution in value of their Private Information; compromise and continuing publication of their Private Information; and are entitled to compensatory, consequential, and incidental damages as a result of the Data Breach.

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

**COUNT VII**  
**Invasion of Privacy–Intrusion Upon Seclusion**  
**(On Behalf of Plaintiffs and the Class)**

277. Plaintiffs re-allege and incorporate each of the foregoing paragraphs as if fully set forth herein.

278. Plaintiffs and the Class had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

279. Defendant owed a duty to its current and former patients and clients, including Plaintiffs and the Class Members, to keep their Private Information confidential.

280. Defendant failed to protect said Private Information and exposed the Private Information of Plaintiffs and the Class Members to unauthorized persons which is now publicly available, including on the dark web, and being fraudulently misused.

281. Defendant allowed unauthorized third parties access to and examination of the Private Information of Plaintiffs and the Class Members, by way of Defendant's failure to protect the Private Information.

282. The unauthorized release to, custody of, and examination by unauthorized third

parties of the Private Information of Plaintiffs and the Class Members is highly offensive to a reasonable person.

283. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class Members disclosed their Private Information to Defendant as a condition of receiving health services, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

284. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiffs' and the Class Members' interests 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.

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

286. Defendant acted with reckless disregard for Plaintiffs' and Class Members' privacy when they allowed improper access to its systems containing Plaintiffs' and Class Members' Private Information.

287. Defendant was aware of the potential of a data breach and failed to adequately safeguard their systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' Private Information.

288. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and

harm to Plaintiffs and the Class Members.

289. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiffs and the Class Members was disclosed to third parties without authorization, causing Plaintiffs and the Class Members to suffer injury and damages as set forth herein, including monetary damages, fraudulent misuse of their Private Information and fraudulent charges; loss of the opportunity to control how their Private Information is used; diminution in value of their Private Information; compromise and continuing publication of their Private Information; and are entitled to compensatory, consequential, and incidental damages as a result of the Data Breach.

290. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class Members.

**COUNT VIII**  
**Violation of the Iowa Consumer Fraud Act ("ICFA")**  
**Iowa Code § 714h.3, 714h.5**

291. Plaintiffs re-allege and incorporate each of the foregoing paragraphs as if fully set forth herein.

292. The ICFA prohibits a person or entity from engaging:

...in a practice or act the person knows or reasonably should know is an unfair practice, deception, fraud, false pretense, or false promise, or the misrepresentation, concealment, suppression, or omission of a material fact, with the intent that others rely upon the unfair practice, deception, fraud, false pretense, false promise,

misrepresentation, concealment, suppression, or omission in connection with the advertisement [and/or] sale[.]

Iowa Code § 714H.3(1).

293. The Iowa Code defines an unfair practice as “an act or practice which causes substantial, unavoidable injury to consumer that is not outweighed by any consumer or competitive benefits which the practice produces.” Iowa Code § 714.16(1)(n).

294. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce.

295. While involved in trade or commerce, Defendant violated the ICFA, by engaging in unfair, deceptive, and unconscionable business practices including, among other things, by:

- a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of its patients, Plaintiffs and the Class Members or Iowa Class Members, from unauthorized access and disclosure;
- b. Failing to disclose the material fact that its computer systems and data security practices were inadequate to safeguard and protect the Private Information of Defendant’s patients and clients from being compromised, unauthorizedly disclosed, stolen, lost, or misused; and
- a. Failing to disclose the Data Breach to Defendant’s patients in “the most expeditious manner possible and without unreasonable delay” in violation of Iowa Code § 715C.2(1).

296. Defendant knew or should have known that the CarePro computer systems and data security practices were inadequate to safeguard Plaintiffs and Class Members’ or Iowa Class Members’ Private Information entrusted to it, and that risk of a data breach or theft was

highly likely.

297. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

298. Defendant's failures constitute an unfair practice and false, deceptive, and misleading representations regarding the security of CarePro's network and aggregation of Private Information.

299. These unfair practices and misleading representations upon which impacted individuals (including Plaintiffs and Iowa Class Members) relied were material facts (e.g., as to Defendant's adequate protection of Private Information), and consumers (including Plaintiffs and Iowa Class Members) relied on those representations to their detriment.

300. In committing the acts alleged above, Defendant engaged in fraudulent, deceptive, and unfair practices by omitting, failing to disclose, or inadequately disclosing to Defendant's patients and clients that it did not follow industry best practices for the collection, use, and storage of Private Information.

301. As a direct and proximate result of Defendant's fraudulent, deceptive, and unfair practices and omissions, Plaintiffs' and the Iowa Class Members' Private Information was disclosed to third parties without authorization, causing and which will continue to cause them damages.

302. As a direct and proximate result of Defendant's conduct, Plaintiffs and Iowa Class Members have suffered injury and damages as set forth herein, including actual pecuniary/monetary damages, fraudulent misuse of their Private Information and fraudulent charges; loss of the opportunity to control how their Private Information is used; diminution in value of their Private Information; compromise and continuing publication of their Private

Information; and are entitled to actual damages as allowed by Iowa Code § 714H.5(1), as well as reasonable attorneys' fees.

303. Further under Iowa Code § 714H.5(1), Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**COUNT IX**  
**Violation of the Iowa Personal Information Security Breach Protection Act ("PISBPA")**  
**Iowa Code § 715c.2.**  
**(On Behalf of Plaintiffs and the Class)**

304. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

305. The Iowa Personal Information Security Breach Protection Act ("PISBPA") states that:

Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business [...] and that was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security [...] to any consumer whose personal information was included in the information that was breached. The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay consistent with the legitimate needs of law enforcement [...] and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

Iowa Code § 715C.2(1).

306. Defendant is a business that licenses computerized data, which includes personal information, of Plaintiffs and Members of the Class or Iowa Class.

307. As defined by Iowa Code § 715C.1(11)(a)(1-3), "personal information" is defined

as “an individual’s first name or first initial and last name in combination with any one or more of the following[:] social security number, driver’s license number, and financial account information.”

308. Defendant acted as a licensee of the sensitive Private Information in using said information to identify patients and clients, to provide health services to patients, and by storing this valuable and highly sensitive information on its computer systems and network.

309. Defendant became aware of the Data Breach on November 16, 2023, yet shockingly it only began to send out the Breach Notice (Exhibit B) to victims of the breach on or around January 23, 2024.

310. Pursuant to Iowa Code § 715C.2(2), Defendant was required to send notice of the breach to victims “immediately following discovery of such breach of security if a consumer’s personal information was included[.] Though Plaintiffs’ and Class Member’s or Iowa Class Members’ personal information, Private Information, was included in the Data Breach and compromised, Defendant failed to send the requisite “immediate” notice under Iowa law.

311. Because Defendant had actual knowledge of the Data Breach as of November 16, 2023, it had an obligation to disclose the Data Breach in a timely fashion without unreasonable delay. CarePro did not.

312. In failing to timely disclose the Data Breach, Plaintiffs and the Class Members or Iowa Class Members were harmed because they were not able to immediately take precautionary action to prevent and mitigate the effects of identity theft and financial fraud.

313. By failing to disclose the Data Breach in a timely and reasonable manner, Defendant violated Iowa Code §§ 715C.2(1).

314. Pursuant to Iowa Code § 715C.2(9), a violation of this section is considered an

unlawful practice under Iowa Code §§ 714.16(7).

315. As a direct and proximate result of Defendant's violation of the notice requirement under PISBPA, Plaintiffs and Iowa Class Members suffered injury and damages as set forth herein, including monetary damages, fraudulent misuse of their Private Information and fraudulent charges; loss of the opportunity to control how their Private Information is used; diminution in value of their Private Information; compromise and continuing publication of their Private Information.

316. Plaintiffs and Class Members or the Iowa Class Members are entitled to recover actual damages, injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

**COUNT IIX**  
**Unjust Enrichment**  
**(On Behalf of Plaintiffs and the Class)**

1. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

2. This count is pleaded in the alternative to Plaintiffs' breach of implied contract claim above (Count III).

3. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for pharmaceutical services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the pharmaceutical services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

4. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving pharmaceutical services. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

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

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

7. Defendant, however, failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

8. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

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

10. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided

to Defendant.

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

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

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

14. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) Plaintiff Bell's Private Information being disseminated on the dark web, according to Experian (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to

access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

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

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs pray for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

- D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
- i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
  - ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
  - iii. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
  - iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;
  - v. Prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;
  - vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to

- promptly correct any problems or issues detected by such third-party security auditors;
- vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
  - viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
  - ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
  - x. Requiring Defendant to conduct regular database scanning and securing checks;
  - xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
  - xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

- xiii. Requiring Defendant to implement a system of tests to assess its respective patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and
- xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
- xvii. 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.

- E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;
- G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- H. For an award of punitive damages, as allowable by law;
- I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- J. Pre- and post-judgment interest on any amounts awarded; and
- K. Such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMANDED**

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

Dated: July 25, 2024

Respectfully submitted,

*/s/ J. Barton Goplerud*

**J. Barton Goplerud, AT0002983**

**Brian O. Marty, AT0011622**

SHINDLER ANDERSON GOPLERUD &  
WEESE P.C.

5015 Grand Ridge Drive, Suite 100

West Des Moines, Iowa 50265-5749

Telephone: (515) 223-4567

Facsimile: (515) 223-8887

Email: goplerud@sagwlaw.com

marty@sagwlaw.com

Gary M. Klinger\*

**MILBERG COLEMAN BRYSON**

**PHILLIPS GROSSMAN PLLC**

227 W. Monroe Street, Suite 2100

Chicago, IL 60606  
Phone: (866) 252-0878  
gklinger@milberg.com

Lynn A. Toops\*  
Amina A. Thomas\*  
COHEN & MALAD, LLP  
One Indiana Square, Suite 1400  
Indianapolis, Indiana 46204  
(317) 636-6481  
[ltoops@cohenandmalad.com](mailto:ltoops@cohenandmalad.com)  
[athomas@cohenandmalad.com](mailto:athomas@cohenandmalad.com)

J. Gerard Stranch, IV \*  
Andrew E. Mize\*  
STRANCH, JENNINGS & GARVEY, PLLC  
The Freedom Center  
223 Rosa L. Parks Avenue, Suite 200  
Nashville, Tennessee 37203  
(615) 254-8801  
(615) 255-5419 (facsimile)  
[gstranch@stranchlaw.com](mailto:gstranch@stranchlaw.com)  
[amize@stranchlaw.com](mailto:amize@stranchlaw.com)

Samuel J. Strauss\*  
Raina C. Borrelli\*  
STRAUSS BORRELLI PLLC  
One Magnificent Mile  
980 N Michigan Avenue, Suite 1610  
Chicago IL, 60611  
Telephone: (872) 263-1100  
Facsimile: (872) 263-1109  
[sam@straussborrelli.com](mailto:sam@straussborrelli.com)  
[raina@straussborrelli.com](mailto:raina@straussborrelli.com)

Roxanne Conlin  
ROXANNE CONLIN & ASSOCIATES, P.C.  
3721 SW 61st Street, Suite C  
Des Moines, Iowa 50321  
(515)283-1111  
[roxanne@roxanneconlinlaw.com](mailto:roxanne@roxanneconlinlaw.com)

*Attorneys For Plaintiff and the Proposed Class*

*\*Pro Hac Vice Application Forthcoming*