

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
SEATTLE DIVISION**

ALICIA BEREND, on behalf of herself and all  
others similarly situated,

Plaintiff,

v.

PROLIANCE SURGEONS, INC., P.S.,

Defendant.

Case No. 2:23-cv-01824

**CLASS ACTION COMPLAINT  
DEMAND FOR JURY TRIAL**

Alicia Berend (“Plaintiff”), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Proliance Surgeons, Inc., P.S. (“Proliance Surgeons” or “Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel’s investigations, and facts of public record.

**NATURE OF ACTION**

1  
2 1. Defendant is a health care provider with over 100 locations in Washington and  
3 over 800,000 patients per year.<sup>1</sup> As such, Defendant stores a litany of highly sensitive personal  
4 identifiable information (“PII”) and protected health information (“PHI”)—together “PII/PHI”—  
5 about its current and former patients.

6 2. This class action arises from Defendant’s *continued* failure to protect its patients’  
7 highly sensitive data.

8 3. Four years ago, Defendant’s data systems were hacked.<sup>2</sup> Defendant apologized  
9 and promised to upgrade its data security.<sup>3</sup>

10 4. But that hacking was not an isolated incident—rather, it was simply part and parcel  
11 of Defendant’s pattern of negligence data security.

12 5. Because in 2023, Defendant experienced a *second* data breach. This class action  
13 arises from that second data breach (the “Data Breach”).

14 6. Plaintiff is a Data Breach victim, having received a breach notice—attached as  
15 Exhibit A. She brings this class action on behalf of herself, and all others harmed by Defendant’s  
16 misconduct.

17 7. The exposure of one’s PII/PHI to cybercriminals is a bell that cannot be unrung.  
18 Before this data breach, the private information of Defendant’s patients was exactly that—private.  
19 Not anymore. Now, their private information is forever exposed and unsecure.

**PARTIES**

20  
21 8. Plaintiff, Alicia Berend, is natural person and citizen of Washington. She resides  
22 in Bellevue, Washington where she intends to remain.

23  
24  
25 <sup>1</sup> *Why Proliance Surgeons*, PROLIANCE SURGEONS, <https://proliancesurgeons.com/why-proliance-surgeons/> (last visited Nov. 27, 2023).

26 <sup>2</sup> *Notice of Data Security Incident*, PROLIANCE SURGEONS, <https://proliancesurgeons.com/wp-content/uploads/2020/12/Proliance-Website-Substitute-Notice.pdf> (last visited Nov. 27, 2023).

27 <sup>3</sup> *Id.*

1 9. Defendant, Proliance Surgeons, Inc., P.S., is a Washington Professional Service  
2 Corporation with its principal place of business at 805 Madison Street Suite 901, Seattle,  
3 Washington 98104.

4 **JURISDICTION AND VENUE**

5 10. This Court has subject matter jurisdiction over this action under the Class Action  
6 Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive  
7 of interest and costs. Members of the proposed Class are citizens of different states than  
8 Defendant. And there are over 100 putative Class members.

9 11. This Court has personal jurisdiction over Defendant because it is headquartered in  
10 Washington, regularly conducts business in Washington, and has sufficient minimum contacts in  
11 Washington.

12 12. Venue is proper in this Court because Defendant’s principal office is in this  
13 District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff’s  
14 claims occurred in this District.

15 **BACKGROUND**

16 ***Defendant Collected and Stored the PII/PHI of Plaintiff and the Class***

17 13. Defendant is a health care provider with over 100 locations in Washington.<sup>4</sup> It  
18 advertises “400 providers, including over 180 board-certified physicians.”<sup>5</sup> And Defendant has  
19 “more than 800,000 patients every year.”<sup>6</sup>

20 14. As part of its business, Defendant receives and maintains the PII/PHI of thousands  
21 of its current and former patients.

22 15. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard  
23 the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and  
24 Class members themselves took reasonable steps to secure their PII/PHI.

25 \_\_\_\_\_  
26 <sup>4</sup> *Why Proliance Surgeons*, PROLIANCE SURGEONS, <https://proliancesurgeons.com/why-proliance-surgeons/> (last visited Nov. 27, 2023).

27 <sup>5</sup> *Id.*

<sup>6</sup> *Id.*

1 16. Under state and federal law, businesses like Defendant have duties to protect  
2 patients' PII/PHI and to notify them about breaches.

3 17. Defendant recognizes these duties. For example, in its "Privacy Policy,"  
4 Defendant declares that:

5 a. "Proliance is committed to honoring the privacy of individuals."<sup>7</sup>

6 b. "Proliance will not disclose any personal information obtained through the  
7 Proliance site."<sup>8</sup>

8 18. Furthermore, via its "Notice of Privacy Practices," Defendant promises its patients  
9 that:

10 a. "Proliance Surgeons, Inc., P.S. is committed to protecting the  
11 confidentiality of your health information."<sup>9</sup>

12 b. "We are required by law to maintain the privacy of your Protected Health  
13 Information (commonly called PHI), even in electronic format, and to  
14 notify you following a breach of unsecured PHI."<sup>10</sup>

15 c. "We are also required to . . . abide by the practices of this current  
16 Notice."<sup>11</sup>

17 d. "This Notice applies to all Proliance Surgeons providers and facilities that  
18 provide health care to you."<sup>12</sup>

19 e. "Certain uses and disclosures of your protected health information will be  
20 made only with your written authorization. . . . These uses and disclosures  
21  
22

---

23 <sup>7</sup> *Disclaimer*, PROLIANCE SURGEONS, <https://proliancesurgeons.com/resource/disclaimer/> (last  
24 visited Nov. 27, 2023).

25 <sup>8</sup> *Id.*

26 <sup>9</sup> *Policies*, PROLIANCE SURGEONS, <https://proliancesurgeons.com/resource/policies/> (last visited  
27 Nov. 27, 2023).

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

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



1 include uses and disclosures not outlined in this Notice and sale of health  
2 information.”<sup>13</sup>

3 19. And again, Defendant declares that “[a]t Proliance, we’re committed to  
4 maintaining the privacy of your health information.”<sup>14</sup>

5 20. Elsewhere, Defendant promises that the software it uses “provides industry-  
6 leading privacy and security for our patients’ data.”<sup>15</sup>

7 ***Defendant’s Pattern of Negligence***

8 21. Unfortunately, Defendant’s Data Breach is not an isolated incident—rather, it is  
9 simply part and parcel of Defendant’s pattern of negligence data security.

10 22. After all, this Data Breach is the *second time* that Defendant experienced a data  
11 breach within the past several years.<sup>16</sup>

12 23. For over *seven months*—starting on November 13, 2019, and ending on June 24,  
13 2020—Defendant’s data systems were hacked.<sup>17</sup>

14 24. This data breach exposed the names, zip codes, and payment card information of  
15 Defendant’s patients.<sup>18</sup>

16 25. In response, Defendant declared that “we deeply regret any worry or  
17 inconvenience that this [data breach] may cause you” and “we take information privacy and  
18 security very seriously.”<sup>19</sup>

19 26. Moreover, Defendant promised that it would use “enhanced security measures to  
20 prevent similar incidents in the future.”<sup>20</sup>

21 \_\_\_\_\_  
22 <sup>13</sup> *Id.*

23 <sup>14</sup> *Medical Records*, PROLIANCE SURGEONS, <https://proliancesurgeons.com/resource/medical-records/> (last visited Nov. 27, 2023).

24 <sup>15</sup> *Phreesia FAQ*, PROLIANCE SURGEONS, <https://proliancesurgeons.com/resource/phreesia-faq/> (last visited Nov. 27, 2023).

25 <sup>16</sup> *Notice of Data Security Incident*, PROLIANCE SURGEONS, <https://proliancesurgeons.com/wp-content/uploads/2020/12/Proliance-Website-Substitute-Notice.pdf> (last visited Nov. 27, 2023).

26 <sup>17</sup> *Id.*

27 <sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

1 ***Defendant’s Data Breach***

2 27. On or around February 11, 2023, Defendant was hacked.<sup>21</sup>

3 28. Worryingly, Defendant has admitted that “systems and files were encrypted.”<sup>22</sup>

4 29. And worse yet, Defendant has confirmed that the “unauthorized access resulted in  
5 the *removal* of a limited number of files.”<sup>23</sup>

6 30. On May 24, 2023—one-hundred and two days *after* the Data Breach—Defendant  
7 realized that it had exposed its current and former patients’ highly sensitive PII/PHI including:

- 8 a. names;
- 9 b. Social Security numbers;
- 10 c. dates of birth;
- 11 d. phone numbers;
- 12 e. email addresses;
- 13 f. driver license numbers;
- 14 g. usernames;
- 15 h. passwords;
- 16 i. identification information;
- 17 j. medical treatment information;
- 18 k. health insurance information; and
- 19 l. financial account numbers.<sup>24</sup>

20 31. Stunningly, Defendant appears to have delayed notifying its current and former  
21 patients until November 21, 2023—a full two-hundred and eighty-three (283) days *after* the Data  
22 Breach.<sup>25</sup>

23 \_\_\_\_\_  
24 <sup>21</sup> *Notice of Network Security Incident*, PROLIANCE SURGEONS,  
<https://proliancesurgeons.com/notice-of-network-security-incident/> (last visited Nov. 27, 2023).

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

26 <sup>23</sup> *Id.* (emphasis added).

27 <sup>24</sup> *Id.*

<sup>25</sup> *Data Breach Report*, MASS. OFFICE CONSUMER AFFAIRS BUS. REG.,  
<https://www.mass.gov/doc/data-breach-report-2023/download> (last visited Nov. 27, 2023).

1           32.     Thus, Defendant kept the Class in the dark—thereby depriving the Class of the  
2 opportunity to try and mitigate their injuries in a timely manner.

3           33.     Currently, the precise number of persons injured is unclear. But upon information  
4 and belief, the size of the putative class can be ascertained from information in Defendant’s  
5 custody and control. And upon information and belief, the putative class is over one hundred  
6 members—as it includes Defendant’s current and former patients.

7           34.     And when Defendant did notify Plaintiff and the Class of the Data Breach,  
8 Defendant acknowledged that the Data Breach created a present, continuing, and significant risk  
9 of suffering identity theft, warning Plaintiff and the Class:

- 10           a.     “review[] financial account statements for any signs of fraudulent  
11 activity;”
- 12           b.     “check[] explanation of benefits statements from health insurance  
13 providers;”
- 14           c.     “plac[e] an initial 1-year ‘fraud alert’ on your credit files;”
- 15           d.     “contact any of the three major credit bureaus;”
- 16           e.     “request a ‘Security Freeze’ on your credit file;”
- 17           f.     “file a police report in your current city of residence;”
- 18           g.     “request your free credit reports by calling 1-877-322-8228 or visiting the  
19 website [www.annualcreditreport.com](http://www.annualcreditreport.com) . . . [then] review them for any  
20 discrepancies . . . [l]ook out for accounts you didn’t open or inquiries from  
21 unauthorized creditors . . . [v]erify that all the information is accurate;”
- 22           h.     “review the ‘explanation of benefits’ statements you receive from your  
23 health insurance company;”
- 24           i.     “request copies of your medical records from February 11, 2023, to the  
25 present;” and  
26  
27

1 j. “[r]equest a current year-to-date report from your insurance company,  
2 detailing all services provided to you as a beneficiary.”<sup>26</sup>

3 35. Defendant failed its duties when its inadequate security practices caused the Data  
4 Breach. In other words, Defendant’s negligence is evidenced by its failure to prevent the Data  
5 Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused  
6 widespread injury and monetary damages.

7 36. Since the breach, Defendant has “enhance[d] our cybersecurity protocols,”  
8 “refine[d] our practices to enhance the security and privacy of personal and protected health  
9 information,” and “implement[ed] measures to reinforce our existing cybersecurity protocols.”<sup>27</sup>

10 37. But this is too little too late. Simply put, these measures—which Defendant now  
11 recognizes as necessary—should have been implemented *before* the Data Breach.

12 38. On information and belief, Defendant failed to adequately train its employees on  
13 reasonable cybersecurity protocols or implement reasonable security measures.

14 39. Further, the Notice of Data Breach shows that Defendant cannot—or will not—  
15 determine the full scope of the Data Breach, as Defendant has been unable to determine precisely  
16 what information was stolen and when.

17 40. Defendant has done little to remedy its Data Breach. True, Defendant has offered  
18 some Class members basic credit monitoring. But upon information and belief, such rudimentary  
19 offerings are wholly insufficient given the scope of the Data Breach.

20 41. Because of Defendant’s Data Breach, the sensitive PII/PHI of Plaintiff and Class  
21 members was placed into the hands of cybercriminals—inflicting numerous injuries and  
22 significant damages upon Plaintiff and Class members.

23  
24  
25  
26 

---

<sup>26</sup> *Notice of Network Security Incident*, PROLIANCE SURGEONS,  
27 <https://proliancesurgeons.com/notice-of-network-security-incident/> (last visited Nov. 27, 2023).

<sup>27</sup> *Id.*

1 42. Upon information and belief, the cybercriminals in question are particularly  
2 sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2)  
3 successfully encrypted files and systems, and (3) actually *removed* sensitive files.<sup>28</sup>

4 43. And as the Harvard Business Review notes, such “[c]ybercriminals frequently use  
5 the dark web—a hub of criminal and illicit activity—to sell data from companies that they have  
6 gained unauthorized access to through credential stuffing attacks, phishing attacks, [or]  
7 hacking.”<sup>29</sup>

8 44. Thus, on information and belief, Plaintiff’s and the Class’s stolen PII/PHI has  
9 already been published—or will be published imminently—by cybercriminals on the dark web.

10 ***Plaintiff’s Experiences and Injuries***

11 45. Plaintiff is a former patient of Defendant—having received medical services from  
12 approximately 2018 to February 2023.

13 46. Thus, Defendant obtained and maintained Plaintiff’s PII/PHI.

14 47. As a result, Plaintiff Alicia Berend was injured by Defendant’s Data Breach.

15 48. As a condition of receiving medical services from Defendant, Plaintiff provided  
16 Defendant with her PII/PHI. Defendant used that PII/PHI to facilitate its provision of medical  
17 services.

18 49. Plaintiff provided her PII/PHI to Defendant and trusted the company would use  
19 reasonable measures to protect it according to Defendant’s internal policies, as well as state and  
20 federal law. Defendant obtained and continues to maintain Plaintiff’s PII/PHI and has a  
21 continuing legal duty and obligation to protect that PII/PHI from unauthorized access and  
22 disclosure.

23 50. Plaintiff reasonably understood that a portion of the funds paid to Defendant would  
24 be used to pay for adequate cybersecurity and protection of PII/PHI.

25 \_\_\_\_\_  
26 <sup>28</sup> *Id.*

27 <sup>29</sup> Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

1 51. Plaintiff received a Notice of Data Breach dated November 20, 2023.

2 52. Thus, on information and belief, Plaintiff’s PII/PHI has already been published—  
3 or will be published imminently—by cybercriminals on the dark web.

4 53. Through its Data Breach, Defendant compromised Plaintiff’s:

- 5 a. name;
- 6 b. Social Security number;
- 7 c. date of birth;
- 8 d. phone number;
- 9 e. health insurance information;
- 10 f. medical record number;
- 11 g. medical diagnoses; and
- 12 h. medical treatment information.

13 54. Plaintiff has *already* suffered from identity theft and fraud. Specifically, Plaintiff  
14 has received emails indicating that someone has used her identity for various out-of-state  
15 activities—e.g., inquiring into properties in Florida.

16 55. Plaintiff has spent—and will continue to spend—significant time and effort  
17 monitoring her accounts to protect herself from identity theft. After all, Defendant directed  
18 Plaintiff to take those steps in its breach notice.

19 56. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in  
20 spam messages and phone calls.

21 57. Plaintiff fears for her personal financial security and worries about what  
22 information was exposed in the Data Breach.

23 58. Because of Defendant’s Data Breach, Plaintiff has suffered—and will continue to  
24 suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond  
25 allegations of mere worry or inconvenience. Rather, Plaintiff’s injuries are precisely the type of  
26 injuries that the law contemplates and addresses.

1           59. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which  
2 violates her rights to privacy.

3           60. Plaintiff suffered actual injury in the form of damages to and diminution in the  
4 value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant  
5 was required to adequately protect.

6           61. Plaintiff suffered imminent and impending injury arising from the substantially  
7 increased risk of fraud, misuse, and identity theft—all because Defendant’s Data Breach placed  
8 Plaintiff’s PII/PHI right in the hands of criminals.

9           62. Because of the Data Breach, Plaintiff anticipates spending considerable amounts  
10 of time and money to try and mitigate her injuries.

11           63. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which,  
12 upon information and belief, remains backed up in Defendant’s possession—is protected and  
13 safeguarded from additional breaches.

14 ***Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft***

15           64. Because of Defendant’s failure to prevent the Data Breach, Plaintiff and Class  
16 members suffered—and will continue to suffer—damages. These damages include, *inter alia*,  
17 monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an  
18 increased risk of suffering:

- 19           a. loss of the opportunity to control how their PII/PHI is used;
- 20           b. diminution in value of their PII/PHI;
- 21           c. compromise and continuing publication of their PII/PHI;
- 22           d. out-of-pocket costs from trying to prevent, detect, and recovery from  
23 identity theft and fraud;
- 24           e. lost opportunity costs and wages from spending time trying to mitigate the  
25 fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting,  
26 and recovering from identify theft and fraud;
- 27           f. delay in receipt of tax refund monies;

1 g. unauthorized use of their stolen PII/PHI; and

2 h. continued risk to their PII/PHI—which remains in Defendant’s  
3 possession—and is thus as risk for futures breaches so long as Defendant  
4 fails to take appropriate measures to protect the PII/PHI.

5 65. Stolen PII/PHI is one of the most valuable commodities on the criminal  
6 information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can  
7 be worth up to \$1,000.00 depending on the type of information obtained.

8 66. The value of Plaintiff and Class’s PII/PHI on the black market is considerable.  
9 Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen  
10 information openly and directly on the “dark web”—further exposing the information.

11 67. It can take victims years to discover such identity theft and fraud. This gives  
12 criminals plenty of time to sell the PII/PHI far and wide.

13 68. One way that criminals profit from stolen PII/PHI is by creating comprehensive  
14 dossiers on individuals called “Fullz” packages. These dossiers are both shockingly accurate and  
15 comprehensive. Criminals create them by cross-referencing and combining two sources of data—  
16 first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone  
17 numbers, emails, addresses, etc.).

18 69. The development of “Fullz” packages means that the PII/PHI exposed in the Data  
19 Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

20 70. In other words, even if certain information such as emails, phone numbers, or  
21 credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data  
22 Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous  
23 operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly  
24 what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact,  
25 including this Court or a jury, to find that Plaintiff and other Class members’ stolen PII/PHI is  
26 being misused, and that such misuse is fairly traceable to the Data Breach.

27



1           71. Defendant disclosed the PII/PHI of Plaintiff and Class members for criminals to  
2 use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed  
3 the PII/PHI of Plaintiff and Class members to people engaged in disruptive and unlawful business  
4 practices and tactics, including online account hacking, unauthorized use of financial accounts,  
5 and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the  
6 stolen PII/PHI.

7           72. Defendant’s failure to promptly and properly notify Plaintiff and Class members  
8 of the Data Breach exacerbated Plaintiff and Class members’ injury by depriving them of the  
9 earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps  
10 to mitigate the harm caused by the Data Breach.

11 ***Defendant Knew—Or Should Have Known—of the Risk of a Data Breach***

12           73. Defendant’s data security obligations were particularly important given the  
13 substantial increase in cyberattacks and/or data breaches in recent years.

14           74. In 2021, a record 1,862 data breaches occurred, exposing approximately  
15 293,927,708 sensitive records—a 68% increase from 2020.<sup>30</sup> Of the 1,862 recorded data breaches,  
16 330 of them, or 17.7% were in the medical or healthcare industry.<sup>31</sup> Those 330 reported breaches  
17 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that  
18 exposed nearly 10 million sensitive records (9,700,238) in 2020.<sup>32</sup>

19           75. Indeed, cyberattacks have become so notorious that the Federal Bureau of  
20 Investigation (“FBI”) and U.S. Secret Service issue warnings to potential targets, so they are  
21 aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller  
22 municipalities and hospitals are attractive to ransomware criminals . . . because they often have  
23  
24  
25

---

26 <sup>30</sup> See *2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022)  
<https://notified.idtheftcenter.org/s/>.

27 <sup>31</sup> *Id.*

<sup>32</sup> *Id.*

1 lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>33</sup>

2 76. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare  
3 organizations experienced cyberattacks in the past year.<sup>34</sup>

4 77. Therefore, the increase in such attacks, and attendant risk of future attacks, was  
5 widely known to the public and to anyone in Defendant’s industry, including Defendant.

6 ***Defendant Failed to Follow FTC Guidelines***

7 78. According to the Federal Trade Commission (“FTC”), the need for data security  
8 should be factored into all business decision-making. Thus, the FTC issued numerous guidelines  
9 identifying best data security practices that businesses—like Defendant—should use to protect  
10 against unlawful data exposure.

11 79. In 2016, the FTC updated its publication, *Protecting Personal Information: A*  
12 *Guide for Business*. There, the FTC set guidelines for what data security principles and practices  
13 businesses must use.<sup>35</sup> The FTC declared that, *inter alia*, businesses must:

- 14 a. protect the personal customer information that they keep;
- 15 b. properly dispose of personal information that is no longer needed;
- 16 c. encrypt information stored on computer networks;
- 17 d. understand their network’s vulnerabilities; and
- 18 e. implement policies to correct security problems.

19 80. The guidelines also recommend that businesses watch for the transmission of large  
20 amounts of data out of the system—and then have a response plan ready for such a breach.

21 81. Furthermore, the FTC explains that companies must:

22 \_\_\_\_\_  
23 <sup>33</sup> Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18,  
24 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

25 <sup>34</sup> See Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov.  
26 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack> (last visited Sept. 11, 2023).

27 <sup>35</sup> *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) [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).

- 1 a. not maintain information longer than is needed to authorize a transaction;
- 2 b. limit access to sensitive data;
- 3 c. require complex passwords to be used on networks;
- 4 d. use industry-tested methods for security;
- 5 e. monitor for suspicious activity on the network; and
- 6 f. verify that third-party service providers use reasonable security measures.

7 82. The FTC brings enforcement actions against businesses for failing to protect  
8 customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and  
9 appropriate measures to protect against unauthorized access to confidential consumer data—as  
10 an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),  
11 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must  
12 take to meet their data security obligations.

13 83. In short, Defendant’s failure to use reasonable and appropriate measures to protect  
14 against unauthorized access to patients’ data constitutes an unfair act or practice prohibited by  
15 Section 5 of the FTCA, 15 U.S.C. § 45.

16 ***Defendant Failed to Follow Industry Standards***

17 84. Several best practices have been identified that—at a *minimum*—should be  
18 implemented by businesses like Defendant. These industry standards include: educating all  
19 employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-  
20 malware software; encryption (making data unreadable without a key); multi-factor  
21 authentication; backup data; and limiting which employees can access sensitive data.

22 85. Other industry standard best practices include: installing appropriate malware  
23 detection software; monitoring and limiting the network ports; protecting web browsers and email  
24 management systems; setting up network systems such as firewalls, switches, and routers;  
25 monitoring and protection of physical security systems; protection against any possible  
26 communication system; and training staff regarding critical points.

1 86. Defendant failed to meet the minimum standards of any of the following  
2 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation  
3 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,  
4 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  
5 for Internet Security’s Critical Security Controls (CIS CSC), which are all established standards  
6 in reasonable cybersecurity readiness.

7 87. These frameworks are applicable and accepted industry standards. And by failing  
8 to comply with these accepted standards, Defendant opened the door to the criminals—thereby  
9 causing the Data Breach.

10 ***Defendant Violated HIPAA***

11 88. HIPAA circumscribes security provisions and data privacy responsibilities  
12 designed to keep patients’ medical information safe. HIPAA compliance provisions, commonly  
13 known as the Administrative Simplification Rules, establish national standards for electronic  
14 transactions and code sets to maintain the privacy and security of protected health information.<sup>36</sup>

15 89. HIPAA provides specific privacy rules that require comprehensive administrative,  
16 physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI  
17 and PHI is properly maintained.<sup>37</sup>

18 90. The Data Breach itself resulted from a combination of inadequacies showing  
19 Defendant failed to comply with safeguards mandated by HIPAA. Defendant’s security failures  
20 include, but are not limited to:

21  
22  
23  
24 <sup>36</sup> HIPAA lists 18 types of information that qualify as PHI according to guidance from the  
25 Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names,  
26 addresses, any dates including dates of birth, Social Security numbers, and medical record  
27 numbers.

<sup>37</sup> See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308  
(administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312  
(technical safeguards).

- 1 a. failing to ensure the confidentiality and integrity of electronic PHI that it  
2 creates, receives, maintains and transmits in violation of 45 C.F.R. §  
3 164.306(a)(1);
- 4 b. failing to protect against any reasonably-anticipated threats or hazards to  
5 the security or integrity of electronic PHI in violation of 45 C.F.R. §  
6 164.306(a)(2);
- 7 c. failing to protect against any reasonably anticipated uses or disclosures of  
8 electronic PHI that are not permitted under the privacy rules regarding  
9 individually identifiable health information in violation of 45 C.F.R. §  
10 164.306(a)(3);
- 11 d. failing to ensure compliance with HIPAA security standards by  
12 Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- 13 e. failing to implement technical policies and procedures for electronic  
14 information systems that maintain electronic PHI to allow access only to  
15 those persons or software programs that have been granted access rights in  
16 violation of 45 C.F.R. § 164.312(a)(1);
- 17 f. failing to implement policies and procedures to prevent, detect, contain and  
18 correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- 19 g. failing to identify and respond to suspected or known security incidents  
20 and failing to mitigate, to the extent practicable, harmful effects of security  
21 incidents that are known to the covered entity in violation of 45 C.F.R. §  
22 164.308(a)(6)(ii);
- 23 h. failing to effectively train all staff members on the policies and procedures  
24 with respect to PHI as necessary and appropriate for staff members to carry  
25 out their functions and to maintain security of PHI in violation of 45 C.F.R.  
26 § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and  
27

1 i. failing to design, implement, and enforce policies and procedures  
2 establishing physical and administrative safeguards to reasonably  
3 safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

4 91. Simply put, the Data Breach resulted from a combination of insufficiencies that  
5 demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

6 **CLASS ACTION ALLEGATIONS**

7 92. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3),  
8 individually and on behalf of all members of the following class:

9 All individuals residing in the United States whose PII/PHI was  
10 compromised in the Data Breach discovered by Proliance Surgeons  
11 in May 2023, including all those individuals who received notice of  
the breach.

12 93. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries,  
13 any entity in which Defendant has a controlling interest, any Defendant officer or director, any  
14 successor or assign, and any Judge who adjudicates this case, including their staff and immediate  
15 family.

16 94. Plaintiff reserves the right to amend the class definition.

17 95. Certification of Plaintiff's claims for class-wide treatment is appropriate because  
18 Plaintiff can prove the elements of her claims on class-wide bases using the same evidence as  
19 would be used to prove those elements in individual actions asserting the same claims.

20 96. Ascertainability. All members of the proposed Class are readily ascertainable from  
21 information in Defendant's custody and control. After all, Defendant already identified some  
22 individuals and sent them data breach notices.

23 97. Numerosity. The Class members are so numerous that joinder of all Class  
24 members is impracticable. Upon information and belief, the proposed Class includes at least one  
25 hundred members.

1           98. Typicality. Plaintiff's claims are typical of Class members' claims as each arises  
2 from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable  
3 manner of notifying individuals about the Data Breach.

4           99. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's  
5 common interests. her interests do not conflict with Class members' interests. And Plaintiff has  
6 retained counsel—including lead counsel—that is experienced in complex class action litigation  
7 and data privacy to prosecute this action on the Class's behalf.

8           100. Commonality and Predominance. Plaintiff's and the Class's claims raise  
9 predominantly common fact and legal questions—which predominate over any questions  
10 affecting individual Class members—for which a class wide proceeding can answer for all Class  
11 members. In fact, a class wide proceeding is necessary to answer the following questions:

- 12           a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's  
13 and the Class's PII/PHI;
- 14           b. if Defendant failed to implement and maintain reasonable security  
15 procedures and practices appropriate to the nature and scope of the  
16 information compromised in the Data Breach;
- 17           c. if Defendant were negligent in maintaining, protecting, and securing  
18 PII/PHI;
- 19           d. if Defendant breached contract promises to safeguard Plaintiff and the  
20 Class's PII/PHI;
- 21           e. if Defendant took reasonable measures to determine the extent of the Data  
22 Breach after discovering it;
- 23           f. if Defendant's Breach Notice was reasonable;
- 24           g. if the Data Breach caused Plaintiff and the Class injuries;
- 25           h. what the proper damages measure is; and
- 26           i. if Plaintiff and the Class are entitled to damages, treble damages, and or  
27 injunctive relief.





1 107. Defendant owed—to Plaintiff and Class members—at least the following duties  
2 to:

- 3 a. exercise reasonable care in handling and using the PII/PHI in its care and  
4 custody;
- 5 b. implement industry-standard security procedures sufficient to reasonably  
6 protect the information from a data breach, theft, and unauthorized;
- 7 c. promptly detect attempts at unauthorized access;
- 8 d. notify Plaintiff and Class members within a reasonable timeframe of any  
9 breach to the security of their PII/PHI.

10 108. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and  
11 Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is  
12 required and necessary for Plaintiff and Class members to take appropriate measures to protect  
13 their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary  
14 steps to mitigate the harm caused by the Data Breach.

15 109. Defendant also had a duty to exercise appropriate clearinghouse practices to  
16 remove PII/PHI it was no longer required to retain under applicable regulations.

17 110. Defendant knew or reasonably should have known that the failure to exercise due  
18 care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an  
19 unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the  
20 criminal acts of a third party.

21 111. Defendant’s duty to use reasonable security measures arose because of the special  
22 relationship that existed between Defendant and Plaintiff and the Class. That special relationship  
23 arose because Plaintiff and the Class entrusted Defendant with their confidential PII/PHI, a  
24 necessary part of obtaining services from Defendant.

25 112. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate  
26 computer systems and data security practices to safeguard Plaintiff and Class members’ PII/PHI.  
27

1           113. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,”  
2 including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such  
3 as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC  
4 publications and orders promulgated pursuant to the FTC Act also form part of the basis of  
5 Defendant’s duty to protect Plaintiff and the Class members’ sensitive PII/PHI.

6           114. Defendant violated its duty under Section 5 of the FTC Act by failing to use  
7 reasonable measures to protect PII/PHI and not complying with applicable industry standards as  
8 described in detail herein. Defendant’s conduct was particularly unreasonable given the nature  
9 and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of  
10 a data breach, including, specifically, the immense damages that would result to individuals in  
11 the event of a breach, which ultimately came to pass.

12           115. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for  
13 privacy and security practices—as to protect Plaintiff’s and Class members’ PHI.

14           116. Defendant violated its duty under HIPAA by failing to use reasonable measures to  
15 protect its PHI and by not complying with applicable regulations detailed *supra*. Here too,  
16 Defendant’s conduct was particularly unreasonable given the nature and amount of PHI that  
17 Defendant collected and stored and the foreseeable consequences of a data breach, including,  
18 specifically, the immense damages that would result to individuals in the event of a breach, which  
19 ultimately came to pass.

20           117. The risk that unauthorized persons would attempt to gain access to the PII/PHI and  
21 misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable  
22 that unauthorized individuals would attempt to access Defendant’s databases containing the  
23 PII/PHI—whether by malware or otherwise.

24           118. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk  
25 in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class members’  
26 and the importance of exercising reasonable care in handling it.

27

1 119. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiff and  
2 the Class in deviation of standard industry rules, regulations, and practices at the time of the Data  
3 Breach.

4 120. Defendant breached these duties as evidenced by the Data Breach.

5 121. Defendant acted with wanton and reckless disregard for the security and  
6 confidentiality of Plaintiff's and Class members' PII/PHI by:

7 a. disclosing and providing access to this information to third parties and

8 b. failing to properly supervise both the way the PII/PHI was stored, used,  
9 and exchanged, and those in its employ who were responsible for making  
10 that happen.

11 122. Defendant breached its duties by failing to exercise reasonable care in supervising  
12 its agents, contractors, vendors, and suppliers, and in handling and securing the personal  
13 information and PII/PHI of Plaintiff and Class members which actually and proximately caused  
14 the Data Breach and Plaintiff and Class members' injury.

15 123. Defendant further breached its duties by failing to provide reasonably timely  
16 notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused  
17 and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

18 124. Defendant has admitted that the PII/PHI of Plaintiff and the Class was wrongfully  
19 lost and disclosed to unauthorized third persons because of the Data Breach.

20 125. As a direct and traceable result of Defendant's negligence and/or negligent  
21 supervision, Plaintiff and Class members have suffered or will suffer damages, including  
22 monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and  
23 emotional distress.

24 126. And, on information and belief, Plaintiff's PII/PHI has already been published—  
25 or will be published imminently—by cybercriminals on the dark web.

26 127. Defendant's breach of its common-law duties to exercise reasonable care and its  
27 failures and negligence actually and proximately caused Plaintiff and Class members actual,

1 tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by  
2 criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their  
3 PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach  
4 that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages  
5 are ongoing, imminent, immediate, and which they continue to face.

6 **SECOND CAUSE OF ACTION**  
7 **Breach of Implied Contract**  
8 **(On Behalf of Plaintiff and the Class)**

9 128. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

10 129. Plaintiff and Class members were required to provide their PII/PHI to Defendant  
11 as a condition of receiving medical services provided by Defendant. Plaintiff and Class members  
12 provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's medical  
13 services.

14 130. Plaintiff and Class members reasonably understood that a portion of the funds they  
15 paid Defendant would be used to pay for adequate cybersecurity measures.

16 131. Plaintiff and Class members reasonably understood that Defendant would use  
17 adequate cybersecurity measures to protect the PII/PHI that they were required to provide based  
18 on Defendant's duties under state and federal law and its internal policies.

19 132. Plaintiff and the Class members accepted Defendant's offers by disclosing their  
20 PII/PHI to Defendant or its third-party agents in exchange for medical services.

21 133. In turn, and through internal policies, Defendant agreed to protect and not disclose  
22 the PII/PHI to unauthorized persons.

23 134. In its various policies, Defendant represented that they had a legal duty to protect  
24 Plaintiff's and Class Member's PII/PHI.

25 135. Implicit in the parties' agreement was that Defendant would provide Plaintiff and  
26 Class members with prompt and adequate notice of all unauthorized access and/or theft of their  
27 PII/PHI.

1           136. After all, Plaintiff and Class members would not have entrusted their PII/PHI to  
2 Defendant in the absence of such an agreement with Defendant.

3           137. Plaintiff and the Class fully performed their obligations under the implied  
4 contracts with Defendant.

5           138. The covenant of good faith and fair dealing is an element of every contract. Thus,  
6 parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair  
7 dealing, in connection with executing contracts and discharging performance and other duties  
8 according to their terms, means preserving the spirit—and not merely the letter—of the bargain.  
9 In short, the parties to a contract are mutually obligated to comply with the substance of their  
10 contract in addition to its form.

11           139. Subterfuge and evasion violate the duty of good faith in performance even when  
12 an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And  
13 fair dealing may require more than honesty.

14           140. Defendant materially breached the contracts it entered with Plaintiff and Class  
15 members by:

- 16           a. failing to safeguard their information;
- 17           b. failing to notify them promptly of the intrusion into its computer systems  
18           that compromised such information.
- 19           c. failing to comply with industry standards;
- 20           d. failing to comply with the legal obligations necessarily incorporated into  
21           the agreements; and
- 22           e. failing to ensure the confidentiality and integrity of the electronic PII/PHI  
23           that Defendant created, received, maintained, and transmitted.

24           141. In these and other ways, Defendant violated its duty of good faith and fair dealing.

25           142. Defendant's material breaches were the direct and proximate cause of Plaintiff's  
26 and Class members' injuries (as detailed *supra*).

1 143. And, on information and belief, Plaintiff's PII/PHI has already been published—  
2 or will be published imminently—by cybercriminals on the dark web.

3 144. Plaintiff and Class members performed as required under the relevant agreements,  
4 or such performance was waived by Defendant's conduct.

5 **THIRD CAUSE OF ACTION**  
6 **Breach of Fiduciary Duty**  
7 **(On Behalf of Plaintiff and the Class)**

8 145. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

9 146. Given the relationship between Defendant and Plaintiff and Class members, where  
10 Defendant became guardian of Plaintiff's and Class members' PII/PHI, Defendant became a  
11 fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and  
12 Class members, (1) for the safeguarding of Plaintiff and Class members' PII/PHI; (2) to timely  
13 notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete  
14 and accurate records of what information (and where) Defendant did and does store.

15 147. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members  
16 upon matters within the scope of Defendant's relationship with them—especially to secure their  
17 PII/PHI.

18 148. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members  
19 would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI  
20 had they known the reality of Defendant's inadequate data security practices.

21 149. Defendant breached its fiduciary duties to Plaintiff and Class members by failing  
22 to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

23 150. Defendant also breached its fiduciary duties to Plaintiff and Class members by  
24 failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and  
25 practicable period.

1 151. As a direct and proximate result of Defendant's breach of its fiduciary duties,  
2 Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as  
3 detailed *supra*).

4 **FOURTH CAUSE OF ACTION**  
5 **Invasion of Privacy**  
6 **(On Behalf of Plaintiff and the Class)**

7 152. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

8 153. Plaintiff and the Class had a legitimate expectation of privacy regarding their  
9 highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this  
10 information against disclosure to unauthorized third parties.

11 154. Defendant owed a duty to its current and former patients, including Plaintiff and  
12 the Class, to keep this information confidential.

13 155. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class  
14 members' PII/PHI is highly offensive to a reasonable person.

15 156. The intrusion was into a place or thing which was private and entitled to be private.  
16 Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did  
17 so privately, with the intention that their information would be kept confidential and protected  
18 from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such  
19 information would be kept private and would not be disclosed without their authorization.

20 157. The Data Breach constitutes an intentional interference with Plaintiff's and the  
21 Class's interest in solitude or seclusion, either as to their person or as to their private affairs or  
22 concerns, of a kind that would be highly offensive to a reasonable person.

23 158. Defendant acted with a knowing state of mind when it permitted the Data Breach  
24 because it knew its information security practices were inadequate.

25 159. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and  
26 the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation  
27 efforts.

1 160. Acting with knowledge, Defendant had notice and knew that its inadequate  
2 cybersecurity practices would cause injury to Plaintiff and the Class.

3 161. As a proximate result of Defendant's acts and omissions, the private and sensitive  
4 PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure  
5 and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as  
6 detailed *supra*).

7 162. And, on information and belief, Plaintiff's PII/PHI has already been published—  
8 or will be published imminently—by cybercriminals on the dark web.

9 163. Unless and until enjoined and restrained by order of this Court, Defendant's  
10 wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class  
11 since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system  
12 and policies.

13 164. Plaintiff and the Class have no adequate remedy at law for the injuries relating to  
14 Defendant's continued possession of their sensitive and confidential records. A judgment for  
15 monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the  
16 Class.

17 165. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class  
18 members, also seeks compensatory damages for Defendant's invasion of privacy, which includes  
19 the value of the privacy interest invaded by Defendant, the costs of future monitoring of their  
20 credit history for identity theft and fraud, plus prejudgment interest and costs.

21 **FIFTH CAUSE OF ACTION**  
22 **Unjust Enrichment**  
23 **(On Behalf of Plaintiff and the Class)**

24 166. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

26 168. Plaintiff and Class members conferred a benefit upon Defendant. After all,  
27 Defendant benefitted from using their payment and PII/PHI to provide medical services.  
Furthermore, Defendant benefitted from using their PII/PHI to collect payment.



1 169. Defendant appreciated or had knowledge of the benefits it received from Plaintiff  
2 and Class members (or their third-party agents). And Defendant benefited from receiving  
3 Plaintiff's and Class members' payment and PII/PHI, as they was used to provide medical  
4 services.

5 170. Plaintiff and Class members reasonably understood that Defendant would use  
6 adequate cybersecurity measures to protect the PII/PHI that they were required to provide based  
7 on Defendant's duties under state and federal law and its internal policies.

8 171. Defendant enriched itself by saving the costs they reasonably should have  
9 expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

10 172. Instead of providing a reasonable level of security, or retention policies, that would  
11 have prevented the Data Breach, Defendant instead calculated to avoid its data security  
12 obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security  
13 measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate  
14 result of Defendant's failure to provide the requisite security.

15 173. Under principles of equity and good conscience, Defendant should not be  
16 permitted to retain the full value of Plaintiff's and Class members' PII/PHI and payment because  
17 Defendant failed to adequately protect their PII/PHI.

18 174. Plaintiff and Class members have no adequate remedy at law.

19 175. Defendant should be compelled to disgorge into a common fund—for the benefit  
20 of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of  
21 its misconduct.

22 **SIXTH CAUSE OF ACTION**  
23 **Violation of the Washington Consumer Protection Act**  
24 **RCW 19.86.010, *et seq.***  
25 **(On Behalf of Plaintiff and the Class)**

26 176. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.  
27

1           177. The Washington State Consumer Protection Act, RCW 19.86.020 (the “CPA”)  
2 prohibits any “unfair or deceptive acts or practices” in the conduct of any trade or commerce as  
3 those terms are described by the CPA and relevant case law.

4           178. Defendant is a “person” as described in RWC 19.86.010(1).

5           179. Defendant engages in “trade” and “commerce” as described in RWC 19.86.010(2)  
6 in that they engage in the sale of services and commerce directly and indirectly affecting the  
7 people of the State of Washington.

8           180. By virtue of the above-described wrongful actions, inaction, omissions, and want  
9 of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in  
10 unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that  
11 Defendant’s practices were injurious to the public interest because they injured other persons, had  
12 the capacity to injure other persons, and have the capacity to injure other persons.

13           181. Defendant’s failure to safeguard the PII/PHI exposed in the Data Breach  
14 constitutes an unfair act that offends public policy.

15           182. Defendant’s failure to safeguard the PII/PHI compromised in the Data Breach  
16 caused substantial injury to Plaintiff and Class Members. Defendant’s failure is not outweighed  
17 by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable  
18 by consumers.

19           183. Defendant’s failure to safeguard the PII/PHI disclosed in the Data Breach, and its  
20 failure to provide timely and complete notice of that Data Breach to the victims, is unfair because  
21 these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

22           184. In the course of conducting their business, Defendant committed “unfair or  
23 deceptive acts or practices” by, *inter alia*, knowingly failing to design, adopt, implement, control,  
24 direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies,  
25 procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff’s and  
26 Class Members’ PII/PHI, and violating the common law alleged herein in the process. Plaintiff  
27 and Class Members reserve the right to allege other violations of law by Defendant constituting

1 other unlawful business acts or practices. As described above, Defendant’s wrongful actions,  
2 inaction, omissions, and want of ordinary care are ongoing and continue to this date.

3 185. Defendant also violated the CPA by failing to timely notify, and by concealing  
4 from Plaintiff and Class Members, information regarding the unauthorized release and disclosure  
5 of their PII/PHI. If Plaintiff and Class Members had been notified in an appropriate fashion, and  
6 had the information not been hidden from them, they could have taken precautions to safeguard  
7 and protect their PII/PHI and identities.

8 186. Defendant’s above-described wrongful actions, inaction, omissions, want of  
9 ordinary care, misrepresentations, practices, and non-disclosures also constitute “unfair or  
10 deceptive acts or practices” in violation of the CPA in that Defendant’s wrongful conduct is  
11 substantially injurious to other persons, had the capacity to injure other persons, and has the  
12 capacity to injure other persons.

13 187. The gravity of Defendant’s wrongful conduct outweighs any alleged benefits  
14 attributable to such conduct. There were reasonably available alternatives to further Defendant’s  
15 legitimate business interests other than engaging in the above-described wrongful conduct.

16 188. Defendant’s unfair or deceptive acts or practices occurred in its trade or business  
17 and have and injured and are capable of injuring a substantial portion of the public. Defendant’s  
18 general course of conduct as alleged herein is injurious to the public interest, and the acts  
19 complained of herein are ongoing and/or have a substantial likelihood of being repeated.

20 189. As a direct and proximate result of Defendant’s above-described wrongful actions,  
21 inaction, omissions, and want of ordinary care that directly and proximately caused the Data  
22 Breach and their violations of the CPA, Plaintiff and Class Members have suffered, and will  
23 continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*,  
24 (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud—  
25 risks justifying expenditures for protective and remedial services for which they are entitled to  
26 compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII/PHI; (5)  
27 deprivation of the value of their PII/PHI, for which there is a well-established national and

1 international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring  
2 financial accounts, and mitigating damages.

3 190. Unless restrained and enjoined, Defendant will continue to engage in the above-  
4 described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of  
5 themselves and the Class, seek restitution and an injunction prohibiting Defendant from  
6 continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control,  
7 direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies,  
8 procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI  
9 entrusted to it.

10 191. Plaintiff, on behalf of themselves and Class Members, also seek to recover actual  
11 damages sustained by each Class Member together with the costs of the suit, including reasonable  
12 attorney fees. In addition, Plaintiff, on behalf of themselves and Class Members, request that this  
13 Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each  
14 Class Member by three times the actual damages sustained not to exceed \$25,000.00 per Class  
15 Member.

16 **SEVENTH CAUSE OF ACTION**  
17 **Violation of the Washington Data Breach Disclosure Law**  
18 **RCW 19.255.005, *et seq.***  
19 **(On Behalf of Plaintiff and the Class)**

20 192. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

21 193. Under RCW § 19.255.010(2), “[a]ny person or business that maintains  
22 computerized data that includes personal information that the person or business does not own  
23 shall notify the owner or licensee of the information of any breach of the security of the data  
24 immediately following discovery, if the personal information was, or is reasonably believed to  
25 have been, acquired by an unauthorized person.”

26 194. Upon information and belief, this statute applies to Defendant because Defendant  
27 does not own nor license the PII/PHI in question. Instead, the owners and/or licensees of the  
PII/PHI are Plaintiff and the Class.

1           195. Here, the Data Breach led to “unauthorized acquisition of computerized data that  
2 compromise[d] the security, confidentiality, [and] integrity of personal information maintained  
3 by” Defendant, leading to a “breach of the security of [Defendant’s] systems,” as defined by RCW  
4 § 19.255.010.

5           196. Defendant failed to disclose that the PII/PHI—of Plaintiffs and Class Members—  
6 that had been compromised “immediately” upon discovery, and thus unreasonably delayed  
7 informing Plaintiffs and the proposed Class about the Data Breach.

8           197. In fact, Defendant appears to have delayed notifying its current and former patients  
9 until November 21, 2023—a full two-hundred and eighty-three (283) days *after* the Data Breach.

10          198. Thus, Defendant violated the Washington Data Breach Disclosure Law.

11                                   **EIGHTH CAUSE OF ACTION**  
12 **Violation of the Washington Uniform Health Care Information Act (UHCIA)**  
13 **RCW 70.02.005, *et seq.***  
**(On Behalf of Plaintiff and the Class)**

14          199. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

15          200. UHCIA declares that:

16           a.       “Health care information is personal and sensitive information that if  
17                           improperly used or released may do significant harm to a patient’s interests  
18                           in privacy, health care, or other interests.” § 70.02.005(1).

19           b.       “‘In order to retain the full trust and confidence of patients, health care  
20                           providers have an interest in assuring that health care information is not  
21                           improperly disclosed and in having clear and certain rules for the  
22                           disclosure of health care information.’” § 70.02.005(3).

23           c.       “‘It is the public policy of this state that a patient’s interest in the proper use  
24                           and disclosure of the patient’s health care information survives even when  
25                           the information is held by persons other than health care providers.’” §  
26                           70.02.005(4).

1           201. Here, Defendant is a “health care provider” because Defendant “is licensed,  
2 certified, registered, or otherwise authorized by the law of this state to provide health care in the  
3 ordinary course of business or practice of a profession.” § 70.02.010(19).

4           202. Under § 70.02.020, “a health care provider, an individual who assists a health care  
5 provider in the delivery of health care, or an agent and employee of a health care provider may  
6 not disclose health care information about a patient to any other person without the patient's  
7 written authorization.”

8           203. Here, Defendant violated UHCIA because Defendant—via its Data Breach—  
9 disclosed health care information to third parties without patient authorization.

10   **NINTH CAUSE OF ACTION**  
11   **Declaratory Judgment**  
12   **(On Behalf of Plaintiff and the Class)**

13           204. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

14           205. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is  
15 authorized to enter a judgment declaring the rights and legal relations of the parties and to grant  
16 further necessary relief. The Court has broad authority to restrain acts, such as those alleged  
17 herein, which are tortious and unlawful.

18           206. In the fallout of the Data Breach, an actual controversy has arisen about  
19 Defendant’s various duties to use reasonable data security. On information and belief, Plaintiff  
20 alleges that Defendant’s actions were—and *still* are—inadequate and unreasonable. And Plaintiff  
21 and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

22           207. Given its authority under the Declaratory Judgment Act, this Court should enter a  
23 judgment declaring, among other things, the following:

- 24           a. Defendant owed—and continues to owe—a legal duty to use reasonable  
25 data security to secure the data entrusted to it;
- 26           b. Defendant has a duty to notify impacted individuals of the Data Breach  
27 under the common law and Section 5 of the FTC Act;

1 c. Defendant breached, and continues to breach, its duties by failing to use  
2 reasonable measures to the data entrusted to it; and

3 d. Defendant breaches of its duties caused—and continues to cause—injuries  
4 to Plaintiff and Class members.

5 208. The Court should also issue corresponding injunctive relief requiring Defendant  
6 to use adequate security consistent with industry standards to protect the data entrusted to it.

7 209. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury  
8 and lack an adequate legal remedy if Defendant experiences a second data breach.

9 210. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy  
10 at law because many of the resulting injuries are not readily quantified in full and they will be  
11 forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—  
12 while warranted for out-of-pocket damages and other legally quantifiable and provable  
13 damages—cannot cover the full extent of Plaintiff and Class members’ injuries.

14 211. If an injunction is not issued, the resulting hardship to Plaintiff and Class members  
15 far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

16 212. An injunction would benefit the public by preventing another data breach—thus  
17 preventing further injuries to Plaintiff, Class members, and the public at large.

18 **PRAYER FOR RELIEF**

19 Plaintiff and Class members respectfully request judgment against Defendant and that the  
20 Court enter an order:

21 A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class,  
22 appointing Plaintiff as class representative, and appointing her counsel to represent  
23 the Class;

24 B. Awarding declaratory and other equitable relief as necessary to protect the  
25 interests of Plaintiff and the Class;

26 C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the  
27 Class;

- 1 D. Awarding Plaintiff and the Class damages including applicable compensatory,  
2 exemplary, punitive damages, and statutory damages, as allowed by law;  
3 E. Awarding restitution and damages to Plaintiff and the Class in an amount to be  
4 determined at trial;  
5 F. Awarding attorneys' fees and costs, as allowed by law;  
6 G. Awarding prejudgment and post-judgment interest, as provided by law;  
7 H. Granting Plaintiff and the Class leave to amend this complaint to conform to the  
8 evidence produced at trial; and  
9 I. Granting other relief that this Court finds appropriate.

10 **DEMAND FOR JURY TRIAL**

11 Plaintiff demands a jury trial for all claims so triable.  
12  
13

14 Dated: November 27, 2023

By: /s/ Samuel J. Strauss  
Samuel J. Strauss, WSBA #46971  
TURKE & STRAUSS LLP  
613 Williamson St., Suite 201  
Madison, Wisconsin 53703-3515  
Telephone: (608) 237-1775  
Facsimile: (608) 509 4423  
sam@turkestrauss.com

15  
16  
17  
18  
19 *Attorneys for Plaintiff and the Proposed Class*  
20  
21  
22  
23  
24  
25  
26  
27



**— EXHIBIT A —**

Proliance Surgeons  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998



PIZCJW00410750  
ALICIA SHANNON BEREND  
526 172ND AVE NE  
BELLEVUE, WA 98008-4118  
[Barcode]

**IMPORTANT INFORMATION**  
**PLEASE REVIEW CAREFULLY**



November 20, 2023

Dear Alicia:

Proliance Surgeons (“Proliance”) is committed to our patients, their treatment, and their families – as well as protecting the privacy and security of their personal information. We are writing with important information regarding a data security incident that may have affected your personal information. The privacy and security of the information we maintain is of the utmost importance to Proliance Surgeons. We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

Proliance detected that certain systems within our network had been affected by a cybersecurity incident. The incident resulted in the potential unauthorized access and/or acquisition of certain files from the network, which occurred on February 11, 2023.

What We Are Doing

Upon detecting the incident, Proliance commenced an immediate and thorough investigation, contained the network, alerted law enforcement, and notified certain individuals whose personal information was present in the above-mentioned files. As part of our investigation, Proliance engaged third party cybersecurity professionals to investigate the extent of the activity and what, if any, additional individual personal information may have been accessed and/or acquired by an unauthorized party. On May 24, 2023, we discovered that certain additional files involved in the incident could have contained personal information but had not yet identified the specific individuals involved. As a result, we posted a notice to our website about the incident, and included steps individuals could take to protect their personal information. We conducted a detailed and comprehensive review of all the data involved, and determined on September 22, 2023 that your information was present in the additional files potentially accessed and/or acquired by an unauthorized party. We immediately took steps to notify you of the incident and provide you with information to safeguard your personal information.

What Information Was Involved?

The information potentially involved includes your name and Date of Birth, Phone Number, Social Security Number, Medical Record Number, Diagnosis and Treatment Information and Health Insurance Information.

What You Can Do

To protect you from the potential misuse of your information we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally,

PIZCJW0041075010750010210400

we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

This letter also provides other precautionary measures you can take to protect your information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements, explanation of benefits, and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Proliance values your privacy and deeply regrets that this incident has occurred. We take the security of your information very seriously and have taken many additional precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your information. Since detecting the incident, we have reviewed and revised our information security practices, and implemented additional security measures to mitigate the chance of a similar event in the future.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-833-609-3856. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against misuse of your information. The response line is available Monday through Friday, 8:00 am to 8:00 pm Eastern Time, excluding holidays.

Sincerely,

Proliance Surgeons



**OTHER IMPORTANT INFORMATION****1. Enrolling in Complimentary Credit Monitoring.**

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/proliance> and follow the instructions provided. When prompted please provide the following unique code to receive services: V59QLZGNWC

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

**2. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

***Equifax***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/center.html>  
(888) 397-3742

***TransUnion***

Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

**3. Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

***Equifax Security Freeze***

P.O. Box 105788  
Atlanta, GA 30348-5788  
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>  
(888)-298-0045

***Experian Security Freeze***

P.O. Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
(888) 397-3742

***TransUnion Security Freeze***

P.O. Box 160  
Woodlyn, PA 19094  
<https://www.transunion.com/credit-freeze>  
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

**4. Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at [www.annualcreditreport.com](http://www.annualcreditreport.com). Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.





5. **Protecting Your Health Information.**

As a general matter the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits” statement which you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential disclosure (February 11, 2023) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.

6. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

**New York Residents:** You may obtain information about preventing identity theft from the New York Attorney General’s Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

**North Carolina Residents:** You may obtain information about preventing identity theft from the North Carolina Attorney General’s Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov/](http://www.ncdoj.gov/), Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

**Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General’s Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

**Iowa Residents:** You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov), Telephone: 515-281-5164.