John Heenan
HEENAN & COOK
1631 Zimmerman Trail
Billings, MT 59102
Phone: (406) 839-9091
john@lawmontana.com

Attorneys for Plaintiff
**Additional attorneys in signature block*

MONTANA THIRTEENTH JUDICIAL DISTRICT COURT
YELLOWSTONE COUNTY

NICOLE DOWNEY, on behalf of herself and all others similarly situated, Plaintiff, vs. INTERMOUNTAIN PLANNED PARENTHOOD, INC. d/b/a PLANNED PARENTHOOD OF MONTANA, Defendant.	Cause No. DV-56-2025-0000018-NE Brett Linneweber **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff Nicole Downey ("Plaintiff"), brings this Class Action Complaint against Defendant Intermountain Planned Parenthood, Inc. d/b/a Planned Parenthood of Montana ("Defendant"), individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information ("PII") and protected health information ("PHI") of Plaintiff and other similarly situated current and former patients of

Defendant ("Class Members"), including their names, addresses, dates of birth, medical records numbers, health insurance information, provider names, dates of services, diagnosis information, treatment information, and/or prescription information ("Private Information"). *See* Plaintiff Downey's Notification Letter, attached hereto as Exhibit A.

2. On or about August 28, 2024, Defendant learned that its system was subject to unauthorized access ("Data Breach").

3. Defendant conducted an investigation using outside consultants, which concluded on September 6, 2024. Defendant determined between August 24, 2024, and August 28, 2024, files were acquired off its system.[1] Exhibit A.

4. The Data Breach timeline makes clear that Defendant failed to implement reasonable, cybersecurity safeguards as it has a duty to do. For example, the malicious activity began at least by August 24, 2024, yet Defendant did not even notice it until August 28, 2024.[2] If Defendant had implemented appropriate logging, monitoring, and alerting systems, then the cybercriminals likely would not have been able to break into Defendant's information systems, perform noisy reconnaissance activities necessary to identify the location of digital assets, and then exfiltrate those assets all without being caught or even noticed.

5. Moreover, Defendant appears to have been ill-prepared to face the threat of a cyberattack, notwithstanding that such attacks and their resulting harm is imminently foreseeable.

6. The impact to its systems strongly implies that Defendant lacked sufficient cybersecurity incident response and disaster recovery plans, or that the plans it had were not sufficiently tests through the use of tabletop exercises, as is the industry norm.

---

[1] https://www.plannedparenthood.org/uploads/filer_public/01/2a/012a5251-f254-4cfe-b563-333b2e2fb70c/websitenoticeupdated.pdf (last visited Jan. 3, 2024).
[2] *Id.*

7. Notwithstanding that the attack occurred at least by August 24, 2024, Defendant waited until November 5, 2024, to begin notifying its current and former patients of the Data Breach.

8. Defendant's unreasonable and unexplained delays prevented Plaintiff from being able to timely protect herself from the significantly increased risk of harm they must now face for years because of Defendant's disclosure of their Private Information.

9. Plaintiff brings this action on behalf of all persons whose Private Information was compromised because of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) timely warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure its network containing such Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal statutes.

10. Defendant has not provided affected persons or the public any information regarding how the Data Breach occurred or what it is doing to prevent another such incident in the future.

11. Moreover, Defendant's significantly delayed investigation and notification of the Data Breach strongly implies that Defendant lacked a serious and tested cybersecurity incident response plan, which is a core aspect of any reasonable, industry standard cybersecurity program.

12. By failing to implement cybersecurity safeguards, Defendant blatantly disregarded the rights of Plaintiff and the Class Members, including their right to control how their Private Information is disseminated.

13. Because Defendant still maintains Plaintiff's and Class Members' Private Information on its information systems, they have a continuing interest in ensuring that their

information is and remains safe, and they should be entitled to injunctive and other equitable relief.

14. Plaintiff brings this action to hold Defendant accountable for its failures to properly safeguard Plaintiff's and the proposed Class Members' Private Information that it collected, including by requiring Defendant to provide monetary compensation to Plaintiff and the proposed Class Members for this egregious invasion of their privacy, for allowing their Private Information to fall into the hands of cybercriminals and identity thieves, to provide them with compensation and the means to protect themselves against the significant increase in identity theft and financial fraud they must now combat, and to require Defendant to implement the reasonable, industry standard cybersecurity safeguards necessary to protect the Private Information of Plaintiff and the proposed Class Members that Defendant still has in its possession.

15. Indeed, by collecting Plaintiff's and Class Members' Private Information, Defendant had a duty under the common law to implement reasonable, industry standard cybersecurity safeguards, but failed to implement them, including by failing to implement reasonable policies that would have allowed it to timely respond to this Data Breach, and likely including the failure to train its employees to defend against phishing emails, the failure to employ multi-factor authentication, and at least the failure to encrypt Plaintiff's and Class Members' Private Information, given that it was accessed by unauthorized third-parties in unencrypted form. Moreover, the timeline, as explained above, strongly implies that Defendant lacked appropriate logging, monitoring, and alerts systems as well as appropriate cybersecurity incident response and disaster recovery/continuity plans.

16. Because of Defendant's failures, Plaintiff and Class Members have suffered concrete injuries, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the

Data Breach; (iv) loss of benefit of the bargain; (v) experiencing an increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and substantially increased risk of identity theft and financial fraud.

PARTIES

17. Plaintiff Nicole Downey is a former patient of Defendant residing in Yellowstone County, Montana.

18. Defendant Intermountain Planned Parenthood, Inc. d/b/a Planned Parenthood of Montana is a Montana corporation with its principal place of business in Billings, Montana.

19. Defendant conducts substantial business in Montana, where Plaintiff visited Defendant for its services.

20. Defendant "is the leading provider of sexual and reproductive health care in Montana. We've served Montanans and their families for more than 55 years, and are proud to offer safe, trusted care through in-person and telehealth visits across Big Sky Country."[3]

JURISDICTION

21. The Court has general subject matter jurisdiction over this civil action under Mont. Code Ann. § 3-5-302(1)(b).

22. This Court has personal jurisdiction over Defendant because its principal place of business is in Billings, Montana and it maintains a significant operation in this State.

ADDITIONAL FACTUAL ALLEGATIONS

23. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

24. Defendant made promises and representations to Plaintiff and Class Members that

[3] https://www.plannedparenthood.org/planned-parenthood-montana/about (last visited Jan. 3, 2025).

their Private Information would be kept safe and confidential, and that the privacy of that information would be maintained through the implementation of reasonable cybersecurity measures.

25. Plaintiff's and Class Members' Private Information was provided to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

26. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its patients' Private Information safe and confidential.

27. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

Defendant's Data Breach Was Imminently Foreseeable

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

30. Data thieves regularly target institutions like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected Private Information

is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

31. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[4]

32. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members because of a breach.

33. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

34. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

36. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

---

[4] *See* Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), https://notified.idtheftcenter.org/s/.

Value of Personally Identifiable Information

37. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[5] 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."[6]

38. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[7]

39. For example, Private Information can be sold at a price ranging from $40 to $200.[8] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[9]

40. 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 typical 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

---

[5] 17 C.F.R. § 248.201 (2013).
[6] *Id.*
[7] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.
[8] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.
[9] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark.

impossible, to change.

41. 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."[10]

42. 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:

> [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.[11]

Defendant Failed to Comply with FTC Guidelines

43. The 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

44. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines

---

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

[11] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

note that businesses should protect the personal information 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. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into 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.

45. The FTC further recommends that companies not maintain Private 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

46. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

47. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

48. Defendant was at all times fully aware of its obligation to protect the Private Information of consumers under the FTC Act yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, 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 Plaintiff and the Class.

49. Defendant's failure is even more clear given the timeline and notification letters they sent to Plaintiff. Defendant apparently discovered the Data Breach August 28, 2024, but Defendant took until November 5, 2024, to send out notification letters. This unreasonable delay in responding to the Data Breach strongly implies that Defendant lacked a reasonable cybersecurity incident response plan, as is required by industry standards and FTC expectations.

Defendant Failed to Comply with Industry Standards.

50. Experts studying cybersecurity routinely identify institutions that store Private Information like Defendant as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

51. Some industry best practices that should be implemented by institutions dealing with sensitive Private Information, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline, Defendant failed to follow some or all these industry best practices.

52. Other best cybersecurity practices that are standard at large institutions that store

Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach and Defendant's failure to understand how the Data Breach occurred, Defendant failed to follow these cybersecurity best practices.

53. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

54. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Common Injuries & Damages

55. Because 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 Plaintiff and Class Members has materialized and is imminent, and Plaintiff 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); and (d) 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 Plaintiff's and Class Members' Private Information.

The Data Breach Increases Victims' Risk of Identity Theft.

56. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiff's and Class Members' Private Information falling into the hands of identity thieves.

57. The unencrypted Private Information of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the Private Information for the express purpose of conducting financial fraud and identity theft operations.

58. Further, the standard operating procedure for cybercriminals is to use some data to access "fullz packages" of that person to gain access to the full suite of additional Private Information that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.[12]

[12] "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 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 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),

59. 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 to assemble complete dossiers on individuals.

60. 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 Plaintiff's 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.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

61. Because 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 of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

62. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' Private Information is affected.

---

https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

63. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts and health insurance statements for any indication of fraudulent activity, which may take years to detect.

64. These 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 good name and credit record."[13]

65. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[14]

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

66. Upon information and belief, the Private Information appears to have already been posted online, which significantly enhances the risk of harm to Plaintiff and the proposed Class Members that the data will be used to perpetrate identity theft and financial fraud.

---

[13] *See* U.S. Gov't 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.

[14] *See* Fed. Trade Comm'n, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

67. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

68. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Plaintiff Downey's Experience

69. Plaintiff Downey provided her Private Information to Defendant as a condition of receiving services from Defendant.

70. At the time of the Data Breach, Defendant retained Plaintiff Downey's Private Information in its system.

71. Plaintiff Downey's Private Information was compromised in the Data Breach and stolen by notorious identity thieves who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

72. Plaintiff Downey takes reasonable measures to protect her Private Information.

73. Because of the Data Breach, Plaintiff Downey has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She has and will continue to monitor accounts and credit scores and have sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

74. Plaintiff Downey suffered lost time, interference, and inconvenience because of the Data Breach and has experienced stress and anxiety due to increased concerns for the loss of her

privacy.

75. Plaintiff Downey has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals whose mission it is to misuse that data and who has already posted it online.

76. Defendant obtained and continues to maintain Plaintiff Downey's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed because of the Data Breach.

77. Moreover, Defendant's failures have caused a significant invasion of privacy for Plaintiff Downey and the Class.

78. Because of the Data Breach, Plaintiff Downey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. 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.

CLASS ALLEGATIONS

79. Pursuant to the Montana Rules of Civil Procedure 23(b)(1), 23(b)(3), Plaintiff brings this action on behalf of herself and on behalf of all members of the proposed class defined as:

> All individuals residing in the United States whose Private Information was compromised in the Data Breach and to whom Defendant sent an individual notification that they were affected by the Data Breach ("Class").

80. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

81. Plaintiff reserves the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

82. The proposed Class meets the criteria certification under Montana Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

83. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

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

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTC Act;

c. When Defendant learned of the Data Breach;

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

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

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

g. Whether Defendant owed duties to Class Members to safeguard their Private Information;

h. Whether Defendant breached their duties to Class Members to safeguard their Private Information;

i. Whether hackers obtained Class Members' Private Information via the Data Breach;

j. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

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

m. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached contracts it had with its patients, which were made expressly for the benefit of Plaintiff and Class Members;

p. Whether Plaintiff and Class Members are entitled to damages;

q. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

85. Typicality. Plaintiff's claims are typical of those of other Class Members because

Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

87. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated 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.

88. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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, conducting 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.

89. Class certification is also appropriate. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

90. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach, as is evident by Defendant's ability to send those individuals notification letters.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE AND NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

91. Plaintiff incorporates paragraphs through 90 above as if fully set forth herein.

92. Plaintiff and Class Members provided their non-public Private Information to Defendant in connection with and as a condition of receiving services with Defendant.

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

94. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

95. Defendant had duties to employ reasonable security measures under Section 5 of the FTCA, 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.

96. Defendant's duty to use reasonable security measures also arose under the common law, and as informed by the FTC Act, which mandates that Defendant implement reasonable cybersecurity measures.

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

98. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

99. Indeed, Under Mont. Code Ann. § 30-14-1704, security breaches involving the unencrypted information of Montana residents must be disclosed without unreasonable delay.

100. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiff and Class Members 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 is necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties. Defendant breached its duty to adequately disclose under Mont. Code Ann. § 30-14-1704, which constitutes negligence *per se*.

101. Defendant breached its duties, pursuant to the FTC Act, and other applicable standards, and thus was 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 its networks and systems, including by failing to implement reasonable monitoring, logging, and alerting systems such as EDR/XDR, data loss prevention tools, and a centralized security event management system;

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

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

e. Failing to remove Plaintiff's and Class Members' Private Information it was no longer required to retain pursuant to regulations; and

f. Failing to implement a reasonable cybersecurity incident response plan that would have enabled Defendant to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

102. 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 Plaintiff and Class Members.

103. Defendant's violation of the FTC Act also constitutes negligence *per se*, as those provisions are designed to protect individuals like Plaintiff and the proposed Class Members from the harms associated with data breaches.

104. Defendant has admitted that the Private Information of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

105. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

106. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Private Information of Plaintiff and Class Members 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.

107. As a direct and proximate result of Defendant's conduct, Plaintiff 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 time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) 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.

108. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff 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.

109. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff 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.

110. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

111. Given Defendant's failures to implement the proper systems, as defined above, even knowing the ubiquity of the threat of data breaches, Defendant's decision not to invest enough resources in its cyber defenses amounts to gross negligence.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

112. Plaintiff incorporates paragraphs 1 through 111 above as if fully set forth herein.

113. Plaintiff and the proposed Class Members transferred their Private Information to Defendant as a condition of receiving services from Defendant.

114. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information and paid for Defendant's services. In exchange, Defendant should have provided adequate data security for Plaintiff and Class Members and implicitly agreed to do so.

115. Indeed, Defendant held itself out as a business dedicated to protecting the privacy of Plaintiff's and the proposed Class Members' Private Information.

116. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the

form their Private Information as a necessary part of receiving services.

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

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

119. As a direct and proximate result of Defendant's conduct, Plaintiff 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 time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) nominal damages; and (ix) 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 PII.

COUNT III
BREACH OF BAILMENT
(On Behalf of Plaintiff and the Class)

120. Plaintiff incorporates paragraphs 1 through 119 above as if fully set forth herein.

121. Plaintiff conveyed their Private Information to Defendant lawfully as a condition of receiving services with the understanding that Defendant would return or delete their Private Information when it was no longer required.

122. Defendant accepted this Private Information on the implied understanding that Defendant would honor its obligations under federal regulations, state law, and industry standards to safeguard Plaintiff's Private Information and act on the Private Information only within the confines of the purposes for which Defendant collected Plaintiff's Private Information.

123. By accepting Plaintiff's data and storing it on its systems, Defendant had exclusive control over the privacy of Plaintiff's data in that Plaintiff had no control over whether Defendant's copy of Plaintiff's Private Information was protected with sufficient safeguards and indeed only Defendant had that control.

124. By failing to implement reasonable cybersecurity safeguards, as detailed above, Defendant breached this bailment agreement causing harm to Plaintiff in the form of violations of their right to privacy and to self-determination of who had/has access to their Private Information, in the form of requiring them to spend their own valuable time responding to Defendant's failures, and in the form of forcing Plaintiff and the Class to face years of substantially increased risk of identity theft and financial fraud.

COUNT IV
Invasion of Privacy (Intrusion Upon Seclusion and Public Disclosure of Private Facts)
(On Behalf of Plaintiff and the Class)

125. Plaintiff incorporates paragraphs 1 through 124 above as if fully set forth herein.

126. Plaintiff and Class Members took reasonable and appropriate steps to keep their Private Information confidential from the public.

127. Plaintiff's and Class Members' efforts to safeguard their own Private Information were successful, as their Private Information was not known to the public prior to the Data Breach.

128. Plaintiff and Class Members 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.

129. Defendant owed a duty to its patients, including Plaintiff and the proposed Class Members, to keep their Private Information confidential.

130. The unauthorized release of Private Information is highly offensive to any reasonable person.

131. Plaintiff's and Class Members' Private Information is not of legitimate concern to the public.

132. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was private.

133. Defendant publicized Plaintiff's and Class Members' Private Information, by communicating it to cybercriminals who had no legitimate interest in this Private Information and who had the express purpose of monetizing that information by injecting it into the illicit stream of commerce flowing through the dark web and other malicious channels of communication. (e.g., Telegram and Signal).

134. Upon information and belief, Plaintiff's and the Class Members' Private Information is rapidly becoming public knowledge–among the community writ large–due to the nature of the malware attack that procured it, and the identity theft that it is designed for.

135. Moreover, because of the ubiquitous nature of data breaches, especially in the healthcare industry, Defendant was substantially certain that a failure to protect Private Information would lead to its disclosure to unauthorized third parties, including the thousands of waiting identity thieves who are in a special relationship to Plaintiff and the proposed Class Members—in that those identity thieves are precisely the individuals whose aim it is to misuse such Private Information.

136. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that Defendant's inadequate data security measures will likely result in additional data breaches. Plaintiff and Class members have no adequate remedy at law for the injuries that they will sustain in that a judgment for monetary damages will not prevent further invasions of the Plaintiff's and Class members' privacy by Defendant.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

137. Plaintiff incorporates paragraphs 1 through 136 above as if fully set forth herein.

138. This claim is pled in the alternative to the breach of implied contractual duty claim.

139. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information provided to Defendant, along with payment, as a condition of receiving services.

140. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

141. Because of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the value of services with reasonable data privacy and security practices and procedures, and the services without unreasonable data privacy and security practices and procedures that they received.

142. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class Members' monies paid and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the Class Members would not have provided their Private Information, nor paid Defendant, had they known Defendant would not adequately protect their Private Information.

143. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of their misconduct and the Data Breach alleged herein.

PRAYER FOR RELIEF

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

A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class, pursuant to Montana Rule of Civil Procedure 23;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

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

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

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

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

identifying information of Plaintiff and 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 Plaintiff and Class Members;

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

v. prohibiting Defendant from maintaining the Private Information of Plaintiff 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 their security personnel regarding any new or modified procedures; 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;

ix. requiring Defendant to conduct regular database scanning and securing

checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. 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;

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

xiii. 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;

xiv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xv. for a period of 7 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

E. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: January 7, 2025

Respectfully submitted,

/s/ John Heenan

John Heenan
HEENAN & COOK
1631 Zimmerman Trail
Billings, MT 59102
Phone: (406) 839-9091
john@lawmontana.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
1 W Las Olas Blvd., Suite 500
Ft. Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com
Counsel for Plaintiff and the Proposed Class
*Pro Hac Vice Application Forthcoming**