Jaren Wieland, ISB No. 8265
MOONEY WIELAND WARREN
512 W. Idaho St., Suite 103
Boise, ID 83702
t: 208.401.9219
f: 208.401.9218
jaren.wieland.service@mooneywieland.com

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

Counsel for Plaintiff and Proposed Class

**Pro Hac Vice Application Forthcoming*
Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO

Sonna Griffiths, individually and on behalf of all others similarly situated, Plaintiff, vs. **Kootenai Health Inc.**, an Idaho Non-Profit Corporation, Defendant.	Case No. **Class Action Complaint** **Jury Demand**

Plaintiff Sonna Griffiths ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this Class Action Complaint and alleges the following against

Defendant Kootenai Health, Inc. ("Kootenai Health" or "Defendant"), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Data breaches have become entirely too common, and the reason is the lack of attention and resources that companies like the Defendant expend on protecting sensitive information.

2. Plaintiff brings this class action against Kootenai Health for its failure to properly secure Plaintiff's and Class Members' personally identifiable information ("PII") and personal health information ("PHI").

3. Kootenai Health failed to comply with industry standards to protect information systems that contain PII and PHI. Plaintiff seeks, among other things, orders requiring Kootenai Health to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the disclosure (the "Data Breach") in the future.

4. The Private Information compromised in the Data Breach included personally identifiable information of individuals whose Private Information was maintained by Defendant, including Plaintiff.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information, which Defendant required Plaintiff to provide to receive

medical care..

6. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that property in a dangerous condition.

7. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

8. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private

Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and full notice of the Data Breach.

9. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed the Private Information. Had it properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals a period of unimpeded access to the Private Information of Plaintiff and Class Members.

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

11. As a result of the Data Breach, Plaintiff and Class Members are at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages.

12. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiff's and Class Members' Private Information was targeted, accessed, has been misused, and disseminated on the dark web.

13. Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded warnings to mitigate against the imminent risk of future identity theft and financial loss. Such

mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

14. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (g) deprivation of value of their PII; and (h) the continued risk to their sensitive 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 it.

15. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

16. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence and negligence *per se*, (ii) breach of implied contract, (iii) breach of fiduciary duty; and (iv) unjust enrichment.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to

Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

18. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff's and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

19. Plaintiff Sonna Griffiths is an adult individual who at all relevant times has been a citizen and resident of Idaho, and who has been a patient at Kootenai Health in recent years. She was required to give PII and PHI to Kootenai Health as a condition of receiving medical services.

20. Defendant, Kootenai Health, Inc. is a Non-Profit Corporation formed in Idaho, with its principal place of business at 2003 Kootenai Health Way, Coeur d'Alene, Idaho 83814.

21. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

22. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

23. Plaintiff is not aware of ever being part of a data breach involving her PII or PHI and is concerned that it and other private information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including closing her accounts, checking her credit monitoring service, setting up notices and reports and carefully reviewing all her accounts.

24. Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

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

26. Plaintiff 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.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million,

exclusive of interest and costs. The number of class members exceeds 100, some of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

28. This Court has personal jurisdiction over Defendant because it is an Idaho nonprofit corporation that operates and has its principal place of business in this District and conducts substantial business in this District.

29. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant maintains Plaintiff's and Class Members' Private Information in this District and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

The Data Breach

1. On April 3, 2024, after "discover[ing] suspicious activity in its IT network," Defendant released a press statement stating, "We have no evidence that any information has been misused," and "A comprehensive review of the potentially affected data is ongoing and once complete, we will reach out to impacted individuals with more information."[1]

2. Kootenai Health's disclosures are deficient. They do not include basic details concerning the Data Breach, including, but not limited to, why PII and PHI were stored on

[1] Data breach reported at Kootenai Health, Couer d'Alene Press, https://cdapress.com/news/2024/apr/03/data-breach-reported-at-kootenai-health (last visited April 16, 2024)

systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the data was encrypted or otherwise protected, and what Kootenai Health knows about the degree to which the data has been disseminated.

3. Kootenai Health has not nearly disclosed all the details of the Data Breach and its investigation. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, Kootenai Health has taken to secure the PII and PHI still in its possession. Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiff and Class Members' interests, and ensure that Kootenai Health has proper measures in place to prevent similar incidents from occurring in the future.

The Healthcare Sector is a Primary Target for Data Breaches

4. Kootenai Health was on notice that companies in the healthcare industry are susceptible targets for data breaches.

5. Kootenai Health was also on notice that the Federal Bureau of Investigation has been concerned about data security in the healthcare industry. On April 8, 2014, the FBI's Cyber Division issued a Private Industry Notification to companies within the healthcare sector stating that "the healthcare industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." The same

warning specifically noted that "[t]he FBI has observed malicious actors targeting healthcare-related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or PII."[2]

6. The number of reported North American data breaches increased by over 50% in 2021, from 1,080 in 2020[3], to 1,638 in 2021.[4] As a recent report reflects, "[h]ealthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns."[5]

7. At the end of 2018, the healthcare sector ranked second in the number of data breaches among measured sectors and had the highest rate of exposure for each breach.[6] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to

---

[2] Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014), FBI Cyber Division Private Industry Notification (available at https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf) (last accessed Mar. 14, 2023).

[3] *See* Verizon 2021 Data Breach Investigations Report, at 97, https://www.verizon.com/ business/resources/reports/2021-data-breach-investigations-report.pdf (last accessed Mar. 14, 2023).

[4] *See* Verizon 2022 Data Breach Investigations Report, at 83 (available at https://www.verizon.com/ business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf) (last accessed Mar. 14, 2023).

[5] *Id.* at 62.

[6] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center (available at https://www.idtheftcenter.org/2018-data-breaches) (last accessed Mar. 14, 2023).

restore coverage.[7] Almost 50%of the victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. 40% of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy.[8]

8. Healthcare-related breaches have persisted because criminals see electronic patient data as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82% of participating hospital information security leaders reported having a significant security incident in the previous 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[9] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organizations, including credit bureaus, have so much monetizable information stored in their data centers."[10]

---

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) (available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/) (last accessed Mar. 14, 2023).

[8] *Id.*

[9] *2019 HIMSS Cybersecurity Survey* (available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf) (last accessed Mar. 14, 2023).

[10] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Apr. 4, 2019 (available at https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks) (last accessed Mar. 14, 2023).

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

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[11]

10. As a major healthcare provider, Kootenai Health knew, or should have known, the importance of safeguarding the patients' PII and PHI entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on Kootenai Health patients because of a breach. Kootenai Health failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Kootenai Health Stores Plaintiff and Class Members' PII and PHI

11. Kootenai Health obtains and stores a massive amount of its patients' PII and PHI. As a condition of engaging in health services, Kootenai Health requires that patients entrust it with highly confidential PII and PHI.

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

---

[11] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019) (available at https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals) (last visited Mar. 14, 2023).

13. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and, as Kootenai Health's current and former patients, they rely on Kootenai Health to keep this information confidential and securely maintained, and to make only authorized disclosures of this information.

PII and PHI are Valuable and Subject to Unauthorized Disclosure

14. Kootenai Health was aware that the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

15. PII and PHI are valuable commodities to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[12] Indeed, a robust illegal market exists in which criminals openly post stolen PII and PHI on multiple underground websites, commonly referred to as the "dark web." PHI can sell for as much as $363 on the dark web, according to the Infosec Institute.[13]

16. PHI is particularly valuable because criminals can use it to target victims with frauds and swindles that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

---

[12] Federal Trade Commission, What To Know About Identity Theft (available at https://consumer.ftc.gov/articles/what-know-about-identity-theft) (last accessed Mar. 14, 2023).

[13] Center for Internet Security, *Data Breaches: In the Healthcare Sector* (available at https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/) (last accessed Mar. 14, 2023).

17. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's PHI is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[14]

18. The ramifications of Kootenai Health's failure to keep its patients' PII and PHI secure are long-lasting and severe. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for months or even years thereafter.

19. Further, criminals often trade stolen PII and PHI for years following a breach. Cybercriminals can post stolen PII and PHI on the internet, thereby making such information publicly available.

20. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [15] This gives thieves ample time to seek multiple treatments under the victim's name. 40% of consumers found out they were

[14] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, Kaiser Health News (Feb. 7, 2014) (available at https://khn.org/news/rise-of-indentity-theft/) (last accessed Mar. 14, 2023).

[15] *See* Medical ID Theft Checklist (available at https://www.identityforce.com/blog/medical-id-theft-checklist-2) (last accessed Mar. 14, 2023).

a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[16]

21. Kootenai Health knew, or should have known, the importance of safeguarding its patients' PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Kootenai Health patients because of a breach. Kootenai Health failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

The Data Breach Exposed Plaintiff and Class Members to Identity Theft and Out-of-Pocket Losses

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

23. Despite all the publicly available knowledge of known and foreseeable consequences of the disclosure of PII and PHI, Kootenai Health's policies and practices with respect to maintaining the security of its patients' PII and PHI were reckless, or at the very least, negligent.

24. In virtually all contexts, the expenditure of time has consistently been recognized as compensable, and for many people, it is the basis on which they are compensated.

[16] Experian, The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches (available at https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf) (last accessed Mar. 14, 2023).

Plaintiff and Class Members should be compensated for the time they have expended because of Kootenai Health's misfeasance.

25. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[17]

26. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer financial loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their PII and PHI;

b. identity theft and fraud resulting from the theft of their PII and PHI;

c. costs associated with the detection and prevention of identity theft;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit

[17] 2014 LexisNexis True Cost of Fraud Study (available at https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf) (last accessed Mar. 14, 2023).

monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

g. the continued imminent injury flowing from potential fraud and identify theft posed by their PII and PHI being in the possession of one or more unauthorized third parties.

Kootenai Health's Lax Security Violates HIPAA

27. Kootenai Health had a non-delegable duty to ensure that all PHI it collected and stored was secure.

28. Kootenai Health is bound by HIPAA (*see* 45 C.F.R. § 160.102) and, as a result, is required to comply with the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R Part 160 and Part 164, Subparts A and E, and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

29. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. See 45 C.F.R. § 160.103.

30. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

31. HIPAA requires that Kootenai Health implement appropriate safeguards for this information.

32. Despite these requirements, Kootenai Health failed to comply with its duties under HIPAA and its own Privacy Practices. In particular, Kootenai Health failed to:

a. maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. adequately protect Plaintiff and Class Members' PHI;

c. ensure the confidentiality and integrity of electronic PHI created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. ensure compliance with the electronic PHI security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. train all members of its workforce effectively on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their responsibilities and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b).

33. Kootenai Health failed to comply with its duties under HIPAA despite being aware of the risks associated with unauthorized access to Plaintiff and Class Members' PHI.

Kootenai Health Violated FTC Guidelines

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

35. The FTC has promulgated several guides for businesses that reflect 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.[18]

[18] Federal Trade Commission, Start With Security: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last accessed Mar. 14, 2023).

36. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses.[19] The guidelines reflect that businesses should protect the PII that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

37. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to confidential data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[20]

38. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

39. Kootenai Health failed to properly implement basic data security practices. Kootenai Health's failure to employ reasonable and appropriate measures to protect against

[19] Federal Trade Commission, Protecting Personal Information: A Guide for Business (available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed Mar. 14, 2023).

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

unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

40. Kootenai Health was at all times fully aware of its obligation to protect its patients' PII and PHI because of its position as a healthcare provider. Kootenai Health was also aware of the significant repercussions that would result from its failure to do so.

CLASS ALLEGATIONS

30. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose Private Information was compromised in the Defendant's Data Breach disclosed on April 2, 2024.

31. Excluded from the Classes is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

32. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

41. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. Kootenai Health has disclosed that the Data Breach affected approximately 827,149 patients.

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

b. Whether Defendant was negligent in collecting and storing Plaintiff and Class Members' PII and PHI;

c. Whether Defendant had duties not to disclose the PII and PHI of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff and Class Members' PII and PHI;

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

f. Whether Defendant failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

g. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or punitive damages because of Defendant's wrongful conduct;

i. Whether Plaintiff and Class Members are entitled to restitution because of Defendant's wrongful conduct;

j. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm they face because of the Data Breach; and

k. Whether Plaintiff and Class Members are entitled to identity theft protection for their respective lifetimes.

43. **Typicality:** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII and PHI, like that of every other Class Member, was disclosed by Kootenai Health. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through Defendant's common misconduct. Plaintiff is advancing the same claims and legal theories individually and on behalf of all other Class Members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and Class Members' claims arise from the same operative facts and are based on the same legal theories.

44. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Kootenai Health to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel is competent and experienced in litigating class actions, including extensive experience in data breach litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

45. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Kootenai Health has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Kootenai Health's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Kootenai Health's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

46. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Kootenai Health. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

47. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because

Kootenai Health would necessarily gain an unconscionable advantage in non-class litigation, since Kootenai Health would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by Class Members and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

48. The litigation of Plaintiff's claims is manageable. Kootenai Health's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

49. Adequate notice can be given to Class Members directly using information maintained in Kootenai Health's records.

50. Unless a class-wide injunction is issued, Kootenai Health may continue to maintain inadequate security with respect to the PII and PHI of Class Members, Kootenai Health may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Kootenai Health may continue to act unlawfully as set forth in this Complaint.

COUNT I
NEGLIGENCE
(on behalf of Plaintiff and the Class)

51. Plaintiff re-allege and incorporate by reference herein all the allegations contained in paragraphs 1-50.

52. Kootenai Health knowingly collected, came into possession of, and maintained Plaintiff and Class Members' PII and PHI, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. That duty included, among other things, designing, maintaining, and testing Kootenai Health's security protocols to ensure that Plaintiff and Class Members' Private Information in Defendant's possession was adequately secured and protected, that Plaintiff and Class Members' Private Information on Kootenai Health's networks was not accessible to criminals without authorization, and that Kootenai Health employees tasked with maintaining such information were adequately trained on security measures regarding the security of customers/patients' PII and PHI.

53. As a condition of utilizing Kootenai Health's services, Plaintiff and Class Members were obligated to provide their PII and PHI to Kootenai Health.

54. Plaintiff and Class Members entrusted their PII and PHI to Kootenai Health with the understanding that Kootenai Health would safeguard their information, use their PII and PHI for business purposes only, and not disclose their PII and PHI to unauthorized third parties.

55. Kootenai Health knew or reasonably should have known that a failure to exercise due care in the collecting, storing, and using Plaintiff and Class Members' PII and PHI involved an unreasonable risk of harm to Plaintiff and Class Members.

56. Kootenai Health also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff and Class Members' PII and PHI.

57. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of prior data breaches and disclosures prevalent in today's digital landscape, including the explosion of data breaches involving similarly situated healthcare providers.

58. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Kootenai Health knew or should have known of the inherent risks in collecting and storing Plaintiff and Class Members' PII and PHI, the critical importance of providing adequate security of that information, the necessity for encrypting PHI stored on Kootenai Health's systems, and that it had inadequate IT security protocols in place to secure Plaintiff and Class Members' PII and PHI.

59. Kootenai Health's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Kootenai Health's misconduct included, but was not limited to, failure to take the steps and opportunities to prevent the Data Breach as set forth herein.

60. Plaintiff and Class Members had no ability to protect their PII and PHI that was in Kootenai Health's possession.

61. Kootenai Health was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

62. Kootenai Health had, and continues to have, a duty to timely disclose that Plaintiff and Class Members' PII and PHI within its possession was compromised and precisely the type(s) of information that were compromised.

63. Kootenai Health had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class Members' Private Information.

64. Kootenai Health systematically failed to provide adequate security for data in its possession.

65. Kootenai Health, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class Members' PII and PHI within its possession.

66. Kootenai Health, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff and Class Members' PII and PHI.

67. Kootenai Health, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII and PHI within Kootenai Health's possession might have been compromised and precisely the type of information compromised.

68. Kootenai Health breach of duties owed to Plaintiff and Class Members caused Plaintiff and Class Members' PII and PHI to be compromised.

69. But for all of Kootenai Health's acts of negligence detailed above, including allowing cyber criminals to access its systems containing Plaintiff and Class Members' PII and PHI would not have been compromised.

70. Plaintiff never transmitted her own unencrypted PHI over the internet or any other unsecured source.

71. Following the Data Breach, Plaintiff's PHI has been seized by unauthorized third parties who are now free to exploit and misuse that PHI without any ability for Plaintiff to recapture and erase that PHI from further dissemination—Plaintiff's PHI is forever compromised.

72. But for the Data Breach, Plaintiff would not have incurred the loss and publication of her PHI and other injuries.

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

74. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, loss of privacy, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

75. As a result of Kootenai Health's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII and PHI, which is still in the possession of third parties, will be used for fraudulent purposes.

76. Plaintiff seeks the award of actual damages on behalf of herself and the Class.

77. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Kootenai Health to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Kootenai Health to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

COUNT II
NEGLIGENCE PER SE
(on behalf of Plaintiff and the Class)

78. Plaintiff realleges and incorporates by reference herein all the allegations contained in paragraphs 1-50.

79. Pursuant to the HIPAA (42 U.S.C. § 1302d et seq.), the FTC Act, Kootenai Health was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff and Class Members' PHI and PII.

80. Kootenai Health breached its duties by failing to employ industry standard data and cybersecurity measures to ensure its compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

81. It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff and

Class Members' PII and PHI in compliance with applicable laws would result in an unauthorized third-party gaining access to Kootenai Health networks, databases, and computers that stored or contained Plaintiff and Class Members' PII and PHI.

82. Plaintiff and Class Members' PII and PHI constitute personal property that was stolen due to Kootenai Health's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

83. Kootenai Health's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff and Class Members' unencrypted PII and PHI, and Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Kootenai Health's conduct. Plaintiff and Class Members seek damages and other relief as a result of Kootenai Health's negligence.

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiff and the Class)

84. Plaintiff realleges and incorporates by reference herein all the allegations contained in paragraphs 1-50.

85. When Plaintiff and Class Members provided their PII and PHI to Kootenai Health they entered into implied contracts with Kootenai Health, under which Kootenai Health agreed to take reasonable steps to protect Plaintiff and Class Members' PII and PHI, comply with it statutory and common law duties to protect Plaintiff and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

86. Kootenai Health solicited and invited Plaintiff and Class Members to provide their PII and PHI in order to receive healthcare services. Plaintiff and Class Members accepted Kootenai Health's offers and provided their PII and PHI to Kootenai Health.

87. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Kootenai Health's data security practices complied with its statutory and common law duties to adequately protect Plaintiff and Class Members' PII and PHI and to timely notify them in the event of a data breach.

88. Plaintiff and Class Members paid money to Kootenai Health to receive healthcare services. Plaintiff and Class Members reasonably believed and expected that Kootenai Health would use part of those funds to obtain adequate data security. Kootenai Health failed to do so.

89. Plaintiff and Class Members would not have provided their PII and PHI to Kootenai Health had they known that they would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

90. Plaintiff and Class Members fully performed their obligations under their implied contracts with Kootenai Health.

91. Kootenai Health breached its implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff and Class Members' PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach.

92. The losses and damages Plaintiff sustained, include, but are not limited to:

a. Theft of their PII and PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling, and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Kootenai Health with the mutual understanding that Kootenai Health would safeguard Plaintiff and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Kootenai Health's possession and is subject to further

breaches so long as Kootenai Health fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

93. As a direct and proximate result of Kootenai Health's breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT IV
BREACH OF FIDUCIARY DUTY
(on behalf of Plaintiff and the Class)

94. Plaintiff realleges and incorporates by reference herein all the allegations contained in paragraphs 1-50.

95. Kootenai Health has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship, as a consequence of the special relationship of trust and confidence that exists between patients (like Plaintiff and Class Members) and their medical care providers (like Kootenai Health).

96. In light of their special relationship, Kootenai Health has become the guardian of Plaintiff and Class Members' PII and PHI. Kootenai Health has become a fiduciary, created by its undertaking and guardianship of patient PII and PHI, to act primarily for the benefit of its patients, including Plaintiff and Class Members. This duty included the obligation to

safeguard Plaintiff and Class Members' PII and PHI and to timely notify them in the event of a data breach.

97. Kootenai Health breached its fiduciary duties owed to Plaintiff and Class Members by failing to:

a. properly encrypt and otherwise protect the integrity of the system containing Plaintiff and Class Members' PII and PHI;

b. timely notify and/or warn Plaintiff and Class Members of the Data Breach;

c. ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

f. identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

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

h. protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. ensure its compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94);

j. properly use and disclose PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.;

k. effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);

l. design, implement, and enforce policies and procedures establishing physical and administrative safeguards to

reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c); and

m. otherwise failing to safeguard Plaintiff and Class Members' Private Information.

98. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect patient Private Information in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

99. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT V
UNJUST ENRICHMENT
(on behalf of Plaintiff and the Class)

100. Plaintiff realleges and incorporates by reference herein all the allegations contained in paragraphs 1- 50.

101. Plaintiff and Class Members have an interest, both equitable and legal, in their PHI and PII that was conferred upon, collected by, and maintained by Kootenai Health and that was stolen in the Data Breach.

102. Kootenai Health benefitted from the conferral upon it of Plaintiff and Class Members' PII and PHI, and by its ability to retain and use that information. Kootenai Health understood that it so benefitted.

103. Kootenai Health also understood and appreciated that Plaintiff and Class Members' PHI and PII was private and confidential and that its value depended upon Kootenai Health maintaining its privacy and confidentiality.

104. But for Kootenai Health's willingness and commitment to maintain its privacy and confidentiality, that PHI and PII would not have been transferred to and entrusted with Kootenai Health. Further, if Kootenai Health had disclosed that its data security measures were inadequate, Kootenai Health would not have been permitted to continue in operation by regulators and the healthcare marketplace.

105. As a result of Kootenai Health's wrongful conduct as alleged in this Complaint (including, among other things, its failure to employ adequate data security measures, its continued maintenance and use of Plaintiff and Class Members' PHI without having adequate data security measures, and its other conduct facilitating the theft of that PHI and PII),

Kootenai Health has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

106. Kootenai Health's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiff and Class Members' sensitive PHI and PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers.

107. Under the common law doctrine of unjust enrichment, it is inequitable for Kootenai Health to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff and Class Members' PHI and PII in an unfair and unconscionable manner. Kootenai Health's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

108. The benefit conferred upon, received, and enjoyed by Kootenai Health was not conferred officiously or gratuitously, and it would be inequitable and unjust for Kootenai Health to retain the benefit.

COUNT VIII
INJUNCTIVE/DECLARATORY RELIEF
(on behalf of Plaintiff and the Class)

109. Plaintiff re-allege and incorporate by reference herein all the allegations contained in paragraphs 1-50.

110. Kootenai Health owes a duty of care to Plaintiff and Class Members requiring it to adequately secure PII and PHI.

111. Kootenai Health still stores Plaintiff and Class Members' PII and PHI.

112. Since the Data Breach, Kootenai Health has announced no specific changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent similar incidents from occurring in the future.

113. Kootenai Health has not satisfied its legal duties to Plaintiff and Class Members.

114. Actual harm has arisen in the wake of the Data Breach regarding Kootenai Health's duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and PHI, and Kootenai Health's failure to address the security failings that led to that exposure.

115. Plaintiff, therefore, seek a declaration: (a) that Kootenai Health existing security measures do not comply with its duties of care to provide adequate security; and (b) that to comply with its duties of care, Kootenai Health must implement and maintain reasonable security measures, including, but not limited to, the following:

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

b. ordering that Kootenai Health engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Kootenai Health audit, test, and train its security personnel regarding any new or modified procedures;

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

e. ordering that Kootenai Health purge, delete, and destroy in a reasonably secure manner patient data not necessary for its provision of services;

f. ordering that Kootenai Health conduct regular computer system scanning and security checks;

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

h. ordering Kootenai Health to meaningfully educate its current, former, and prospective patients about the threats they face because of the loss of their PHI to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, pray for relief as follows:

a. for an Order certifying the Class as defined herein, and appointing Plaintiff and her counsel to represent the Class;

b. for equitable relief enjoining Kootenai Health - from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

c. for equitable relief compelling Kootenai Health to use appropriate cyber security methods and policies with respect to PII and PHI collection, storage, and protection, and to disclose with specificity to Class Members the types of PII and PHI compromised;

d. for an award of damages, , as allowed by law in an amount to be determined;

e. for an award of attorney fees, costs, and litigation expenses, as allowed by law;

f. for prejudgment interest on all amounts awarded; and

g. such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a trial by jury on all issues so triable.

Dated April 19, 2024

Jaren Wieland, ISB No. 8265
MOONEY WIELAND WARREN
512 W. Idaho St., Suite 103
Boise, ID 83702
t: 208.401.9219
f: 208.401.9218
jaren.wieland.service@mooneywieland.com

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

Counsel for Plaintiff

**Pro Hac Vice Application Forthcoming*

William "Billy" Peerce Howard
THE CONSUMER PROTECTION FIRM, PLLC
401 East Jackson Street, Suite 2340
Truist Place
Tampa, FL 33602
(813) 500-1500
Billy@TheConsumerProtectionFirm.com
Amanda@TheConsumerProtectionFirm.com

Jeff Ostrow*
KOPELOWITZ OSTROW FERGUSON
WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
ostrow@kolawyers.com

**Pro Hac Vice Application Forthcoming*

ClassAction.org
