

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA**

TERESA JOHNSTON,
individually and as parent and
natural guardian of M.J., a
minor, and behalf of all others
similarly situated,

Plaintiffs,

v.

INTEGRIS HEALTH, INC.,

Defendant.

Case No. CIV-24-69-HE

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Teresa Johnston, individually and as parent and natural guardian of M.J., a minor, and on behalf of all other similarly situated individuals (the “Class” or “Class Members,” as defined below), by and through their undersigned counsel, file this Class Action Complaint against Integris Health, Inc. (“Integris” or “Defendant”). Plaintiffs make the following allegations upon information and belief based on, among other things, the investigation of counsel, and review of public documents.

I. NATURE OF THE ACTION

1. Medical and financial records represent the most sensitive information available concerning a person’s private affairs. These records reveal intimate and personal aspects of the human condition, such as illnesses that might carry social stigma and details about substance abuse, family planning and mental health. Congress has passed legislation under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) in order to protect this highly

confidential data, because in the wrong hands, bad actors may target and exploit the most sensitive and vulnerable populations among the public.

2. Plaintiffs bring this class action lawsuit against Integris for its negligent failure to protect and safeguard M.J.'s and the Class's highly sensitive personally identifiable information ("PII") culminating in a massive and preventable data breach (the "Data Breach" or "Breach").

3. Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. This includes names, addresses, Social Security numbers, dates of birth, health insurance information, and other sensitive medical records.

4. As a result of Integris's insufficient data security, cybercriminals easily infiltrated Integris's inadequately protected computer systems and *stole* the PII of M.J. and the Class. In fact, the cybercriminals responsible for the Data Breach have already begun directly extorting victims of the Data Breach. There is no question M.J.'s and the Class's PII is in the hands of cybercriminals who will use their PII for nefarious purposes for the rest of their lives.

5. On or around December 24, 2023, through December 27, 2023, victims of the Data Breach (including Plaintiffs and Class Members) began receiving emails from cybercriminals, cautioning Plaintiffs and Class Members that Integris was breached in November 2023, impacting over 2 million patients.¹

6. Cybercriminals explicitly stated to Plaintiffs and Class Members in the email, "[i]f you are receiving this message, your data have [sic] been compromised."²

7. In this email, cybercriminals admitted highly sensitive information such as "SSN, DOB, Address, Phone, Insurance Information, and Employer Information" were compromised in

¹ See Exhibit 1.

² *Id.*

the Data Breach.³

8. Cybercriminals also threatened Plaintiffs and Class Members that their “data will sell [sic] on the darknet and be used for fraud and identity theft.”⁴

9. What is perhaps most disturbing, however, is that in the email, cybercriminals provided M.J.’s address, telephone number, date of birth, and Social Security number as proof that it had indeed stolen M.J.’s PII from Integrus.⁵

10. Cybercriminals then extorted Plaintiffs and the Class by giving them until January 5, 2024, to click on a dark web link (a Tor extortion site) contained in the email and pay \$50.00 for their stolen PII.⁶ If Plaintiffs and the Class failed to do so, cybercriminals threatened it would sell the entire database to data brokers on January 5, 2024.⁷

11. According to the cybercriminals’ email, its “tor shop allows users to purchase data for fraud. Any buyer can purchase data “exclusively” for 50\$. This gives the buyer exclusive rights on the data and will remove the data from the shop completely. This feature is useful for fraud activity such as identity theft, opening SIM lines, opening bank accounts, taking out loans, and making USA companies. A buyer can also purchase data without exclusive rights for 3\$. In this case, the data will still be listed on the shop. You can remove your data from our shop and protect it from future fraud by purchasing exclusive rights on it (50\$).”⁸

12. The email then gave instructions on how to access the information stolen in the

³ *Id.*

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

Data Breach on the dark web, thus M.J.'s and the Class's PII is available for anyone to access and view.⁹

13. According to the cybercriminals, it contacted Integris after the Breach, but Integris "refused to resolve this issue."¹⁰

14. This disturbing email from the cybercriminals makes it clear that M.J. and the Class are at an imminent risk of fraud and identity theft.

15. It was not until Plaintiffs and the Class were being extorted by cybercriminals that Integris made a public statement regarding the Data Breach.¹¹

16. As a result of Integris's actions, Plaintiffs and the Class Members experienced damages from: (i) theft of their Personal Information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their Personal Information; (iii) loss of value of their Personal Information; (iv) the amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures; (v) Integris's retention of profits attributable to Plaintiffs' and other customers' Personal Information that Integris failed to adequately protect; (vi) economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiffs are now exposed to; (vii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach; and (viii) overpayments of Integris's products and/or services which Plaintiffs purchased.

17. Plaintiffs bring this action individually and on behalf of the Class, seeking

⁹ *Id.*

¹⁰ *Id.*

¹¹ <https://integrisok.com/landing/cyber-event>.

compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

18. Plaintiffs Teresa Johnston and her minor child, M.J. are individuals domiciled in Oklahoma City, Oklahoma. On or about December 27, 2023, Plaintiffs received the email attached hereto as **Exhibit 1**, from cybercriminals, notifying them that M.J.'s name, address, date of birth, and Social Security number, were stolen in the Data Breach and were available for purchase on the dark web.

19. Plaintiffs are both clients of Integris Health, Inc. and both have been required to provide Personal Information to Integris Health, Inc. In this instance, in order for M.J. to obtain healthcare services from Integris Health, Inc., Ms. Johnston was required to provide Private Information to Integris on M.J.'s behalf.

20. Defendant **Integris Health, Inc.** is a domestic not-for-profit corporation incorporated in the state of Oklahoma with its principal place of business located in Oklahoma City, Oklahoma.

III. JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant.

22. This Court has personal jurisdiction over Defendant because Defendant is

incorporated and/or has its principal place of business in Oklahoma; conducts substantial business in Oklahoma through its headquarters, offices, and affiliates; engaged in the conduct at issue here in Oklahoma; and/or otherwise has substantial contacts with Oklahoma and purposely availed itself to the Courts in Oklahoma.

23. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District.

IV. FACTUAL ALLEGATIONS

A. Integris and its Collection of Plaintiffs' and the Class's PII.

24. Integris Health is Oklahoma's largest not-for-profit health network, operating hospitals, clinics, and urgent care throughout the state.¹²

25. Integris employs more than 9,000 people and generates approximately \$1.5 billion in annual revenue.¹³ These statistics make it apparent Integris could have afforded to implement adequate data security prior to the Breach but deliberately chose not to.

26. In the ordinary course of business, Integris receives the PII of individuals, such as Plaintiffs and the Class, from its employees and patients.

27. Integris obtains, collects, uses, and derives a benefit from the PII of Plaintiffs and Class Members. Integris uses the PII it collects to provide services, making a profit therefrom. Integris would not be able to obtain revenue if not for the acceptance and use of Plaintiffs' and the Class's PII.

¹² See <https://www.bleepingcomputer.com/news/security/integris-health-patients-get-extortion-emails-after-cyberattack/>.

¹³ <https://www.zippia.com/integris-health-careers-27390/revenue/>.

28. By collecting Plaintiffs' and the Class's PII, Integris assumed legal and equitable duties to Plaintiffs and the Class to protect and safeguard their PII from unauthorized access and intrusion.

29. Integris recognizes this duty to protect and safeguard Plaintiffs' and the Class's PII and makes the following claim on its website regarding its protection of sensitive data: "[t]he confidentiality, privacy, and security of information within its care are among INTEGRIS Health's highest priorities."¹⁴

30. However, Integris failed to protect Plaintiffs' and the Class's PII.

31. As a result, Plaintiffs' and Class Members' PII was accessed and stolen from Integris's inadequately secured computer network in a massive a preventable Data Breach, as corroborated by the cybercriminals.¹⁵

B. Integris's Massive and Preventable Data Breach.

32. In or around late December 2023, extortion emails were sent to Plaintiffs and the Class by a cybercriminal group who claimed it stole the PII of over 2 million patients in a cyberattack against Integris in November 2023.¹⁶

33. Cybercriminals claim that during the Data Breach, it stole highly confidential information such as Social Security numbers, dates of birth, addresses, phone numbers, insurance information, and employer information was compromised and stolen.¹⁷ It is also apparent it stole

¹⁴ <https://integrisok.com/landing/cyber-event>.

¹⁵ Exhibit 1.

¹⁶ *Id.*; <https://www.bleepingcomputer.com/news/security/integris-health-patients-get-extortion-emails-after-cyberattack/>.

¹⁷ *See* Exhibit 1.

the email addresses of Plaintiffs and the Class.¹⁸

34. Cybercriminals explicitly informed Plaintiffs and the Class in its extortion email that “[i]f you are receiving this message, your data have [sic] been compromised.”¹⁹

35. Cybercriminals also provided a sample of the victim’s stolen data as proof to confirm the cybercriminals had accessed and stolen the victim’s name, address, phone number, date of birth, and Social Security number in the Breach.²⁰

36. Further, the cybercriminals threatened and extorted victims of the Data Breach and relayed the following harrowing message in broken English:

We have contacted Integris Health, but they refuse to resolve this issue. We give you the opportunity to remove your personal data from our databases before we sell the entire database to data brokers on Jan 5 2024. Our tor shop allows users to purchase data for fraud. Any buyer can purchase data “exclusively” for 50\$. This gives the buyer exclusive rights on the data and will remove the data from the shop completely. This feature is useful for fraud activity such as identity theft, opening SIM lines, opening bank accounts, taking out loans, and making USA companies. A buyer can also purchase data without exclusive rights for 3\$. In this case, the data will still be listed on the shop. You can remove your data from our shop and protect it from future fraud by purchasing exclusive rights on it (50\$).

37. The emails include a link to a dark web website (a Tor extortion site) that currently lists the stolen data for approximately 4,674,000 people, including their names, Social Security Numbers, dates of birth, and information about hospital visits.²¹

38. The website contains data added between October 19th and December 24th, 2023, allowing visitors to pay \$50 to delete the data record or \$3 to view it.²² This was a financially

¹⁸ *Id.*

¹⁹ *Id.*

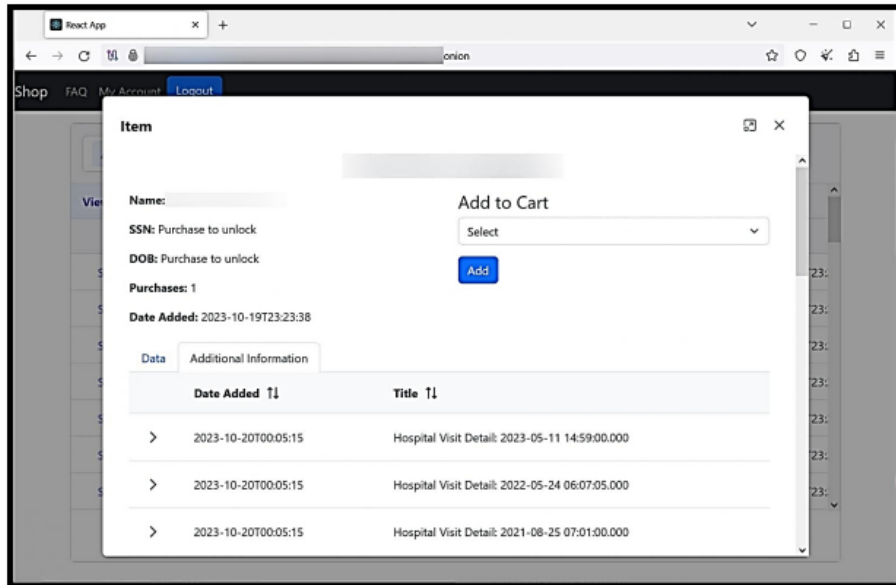
²⁰ *Id.*

²¹ <https://www.bleepingcomputer.com/news/security/integris-health-patients-get-extortion-emails-after-cyberattack/>.

²² *Id.*

motivated Breach that potentially spanned months.

39. Below is a screenshot of the Tor dark web site selling the PII stolen in the Data Breach:²³



40. As threat actors can use the exposed data to conduct identity theft, some patients may be tempted to pay to delete the data.²⁴ However, as previous extortion demands have shown, paying a ransom does not always lead to the actual deletion of data.²⁵

41. On December 24, 2023, Integris publicly announced it experienced a data breach on its website.²⁶

42. According to Integris, on an undisclosed date, Integris discovered unauthorized

²³ *Id.*

²⁴ *Id.*

²⁵ <https://www.bleepingcomputer.com/news/security/scam-psa-ransomware-gangs-dont-always-delete-stolen-data-when-paid/>.

²⁶ <https://integrisok.com/landing/cyber-event>.

activity on certain systems.²⁷

43. After becoming aware of the suspicious activity, Integris initiated an investigation into the nature and scope of the activity.²⁸

44. Integris claims that the investigation determined that certain files may have been accessed by an unauthorized party on November 28, 2023.²⁹

45. However, on December 24, 2023, Integris learned that patients began receiving communications from a group claiming responsibility for the unauthorized access.³⁰

46. Integris Health uploaded a notice to its website on December 24, 2023, finally informing the public of the Data Breach.³¹

47. The images below show portions of the notice that appears on Integris's website:³²

²⁷ *Id.*

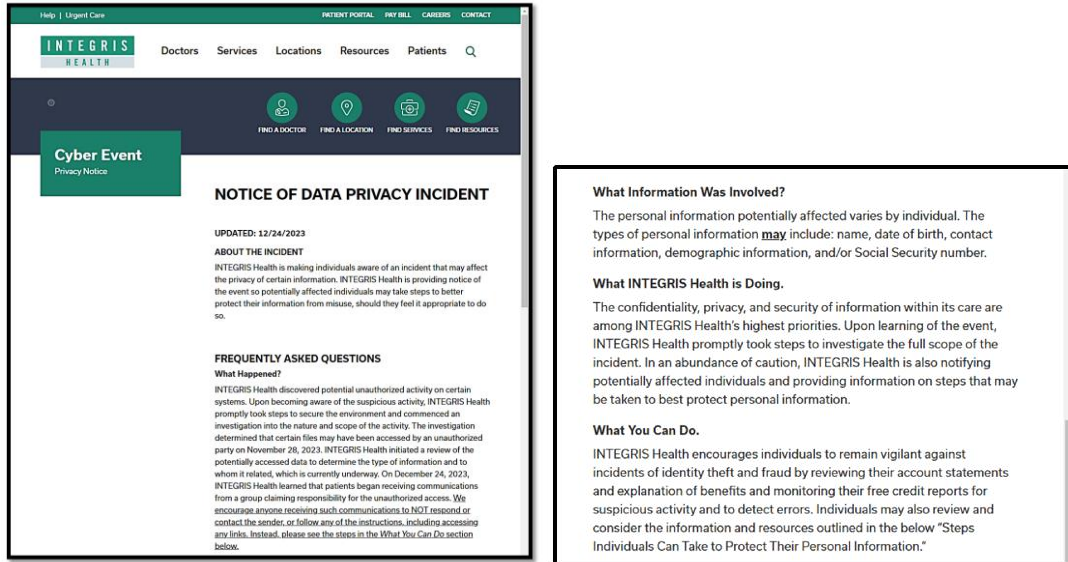
²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ <https://www.hipaajournal.com/integris-health-data-breach/>;
<https://integrisok.com/landing/cyber-event>.

³² *Id.*



48. Integris encouraged anyone receiving communications from the threat actor not to respond or contact the sender, or follow any of the instructions, including accessing any links.³³ But Integris offered no assurance it would retrieve the stolen information.

49. Integris confirmed that the types of PII compromised in the Data Breach varied by individual, but included highly sensitive information such as: names, dates of birth, contact information, demographic information, and/or Social Security numbers.

50. Integris has yet to issue Notice of Data Breach letters to Plaintiffs and the Class, has yet to provide any identity theft protection services for Plaintiffs and the Class, and has not provided Plaintiffs and the Class with any assurance that it retrieved their stolen PII.

51. As evidenced by the cybercriminals' email, Plaintiffs' and the Class's PII is being exploited on the dark web as a result of Integris's failure to adequately protect Plaintiffs' and the Class's PII.

³³ *Id.*

52. Due to Defendant's negligence, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of millions of individuals.

53. All in all, Integris failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access and exploitation.

54. Defendant's actions represent a flagrant disregard of the rights of Plaintiffs and the Class, both as to privacy and property.

55. Integris makes no assurances to Plaintiffs and the Class that it attempted to regain Plaintiffs' and the Class's data from the threat actor or paid the ransom demand.

56. As such, Plaintiffs and the Class are at an imminent and impending risk of identity theft and fraud.

C. Cyber Criminals Will Use Plaintiffs' and the Class's PII to Defraud them.

57. PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

58. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.³⁴

59. For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to

³⁴ *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited Jan. 3, 2024).

other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.³⁵ *Indeed, the cybercriminals highlight in their email how Plaintiffs' and the Class's PII can be misused.*³⁶ These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

60. Social Security numbers are particularly sensitive pieces of personal information.

As the Consumer Federation of America explains:

Social Security number. *This is the most dangerous type of personal information in the hands of identity thieves because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.*³⁷

(Emphasis added.)

61. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.³⁸

62. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running targeted cyberattacks against companies like Integris is to get ransom money and/or information that they can monetize by selling on the black market for use

³⁵ See, e.g., Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/> (last visited Jan. 3, 2024).

³⁶ Exhibit 1.

³⁷ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Jan. 3, 2024).

³⁸ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at <https://www.gao.gov/products/gao-07-737> (last visited Jan. 3, 2024).

in the kinds of criminal activity described herein. Indeed, the cybercriminals' email admits as much.³⁹

63. A Social Security number, date of birth, and full name can sell for \$60 to \$80 on the digital black market.⁴⁰

64. “[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web.”⁴¹

65. These risks are both certainly impending and substantial. As the Federal Trade Commission (“FTC”) has reported, if hackers get access to PII, *they will use it*.⁴²

66. Further, malicious actors often wait months or years to use the Personal Information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen Personal Information, meaning individuals can be the victim of several cybercrimes stemming from a single data breach.

67. The U.S. Government Accountability Office determined that “stolen data may be held for up to a year or more before being used to commit identity theft,” and that “once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for

³⁹ See Exhibit 1.

⁴⁰ Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web* (Nov. 15, 2017), <https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web> (last visited Jan. 3, 2024).

⁴¹ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Jan. 3, 2024).

⁴² Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), <https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info> (last visited Jan. 3, 2024).

years.”⁴³ Moreover, there is often significant lag time between when a person suffers harm due to theft of their Personal Information and when he discovers the harm. Plaintiffs and Class Members will therefore need to spend time and money to continuously monitor their accounts for years to ensure their Personal Information obtained in the Data Breach is not used to harm them. Plaintiffs and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Integris’s Data Breach. In other words, Plaintiffs and Class Members have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Breach.

68. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.⁴⁴

69. With the Data Breach, identity thieves have already started to prey on the Integris breach victims, *i.e.*, the extortion emails, and we can anticipate that this will continue.⁴⁵

70. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.⁴⁶

⁴³ U.S. Gov’t Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm> (last visited Jan. 3, 2024).

⁴⁴ *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/> (last visited Jan. 3, 2024).

⁴⁵ *See* Exhibit 1.

⁴⁶ *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), available at <https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf>.

71. Defendant made no offer of identity monitoring to Plaintiffs and the Class. Even if it did, such coverage would likely be woefully inadequate as it would not be for more than one or two years and would not fully protect Plaintiffs from the damages and harm caused by its failures.

72. The full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

73. Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Integriss's gross negligence.

74. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.⁴⁷ Nor can an identity monitoring service remove personal information from the dark web.⁴⁸

75. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."⁴⁹

76. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have been damaged and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiffs and the Class must now take the time and

⁴⁷ See, e.g., Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), <https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html> (last visited Jan. 3, 2024).

⁴⁸ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Jan. 3, 2024).

⁴⁹ *Id.*

effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

77. Even more seriously is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver’s license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

78. Plaintiffs and the Class were injured as follows: (i) theft of their Personal Information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their Personal Information; (iii) loss of value of their Personal Information; (iv) the lost value of access to Plaintiffs’ and Class Members’ Personal Information permitted by Integris; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Integris’s Data Breach; (vi) Integris’s retention of profits attributable to Plaintiffs’ and Class Members’ Personal Information that Integris failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to Integris for goods and services purchased, as Plaintiffs and Class Members reasonably believed a portion of the price they paid for those goods and services would fund reasonable security measures that would protect their Personal Information, which was not the case; and (x) nominal damages.

79. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' PII.

80. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to Integris is removed from all Integris servers, systems, and files.

81. The notice provided by Integris further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur, stating: INTEGRIS Health encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and explanation of benefits and monitoring their free credit reports for suspicious activity and to detect errors. Individuals may also review and consider the information and resources outlined in the below "Steps Individuals Can Take to Protect Their Personal Information."⁵⁰

82. At Integris's suggestion, Plaintiffs are desperately trying to mitigate the damage that Integris has caused them.

83. Given the kind of PII Integris made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have Plaintiffs' PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.⁵¹

⁵⁰ <https://integrisok.com/landing/cyber-event>.

⁵¹ What happens if I change my Social Security number, LEXINGTON LAW (Aug. 10, 2022), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html> (last visited Jan. 3, 2024).

84. None of this should have happened because the Data Breach was entirely preventable.

D. Defendant was Aware of the Risk of Cyberattacks.

85. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,⁵² Yahoo,⁵³ Marriott International,⁵⁴ Chipotle, Chili's, Arby's,⁵⁵ and others.⁵⁶

86. Integris should certainly have been aware, and indeed was aware,⁵⁷ that it was at risk of a data breach that could expose the PII that it collected and maintained, especially with the rise of healthcare data breaches.

87. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting

⁵² Michael Kassner, Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned, ZDNET (Feb. 2, 2015), <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/> (last visited Jan. 3, 2024).

⁵³ Martyn Williams, Inside the Russian Hack of Yahoo: How They Did It, CSOONLINE.COM (Oct. 4, 2017), <https://www.csoonline.com/article/560623/inside-the-russian-hack-of-yahoo-how-they-did-it.html> (last visited Jan. 3, 2024).

⁵⁴ Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), <https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/> (last Jan. 3, 2024).

⁵⁵ Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), <https://www.cnet.com/news/privacy/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b> (last visited Jan. 3, 2024).

⁵⁶ See, e.g., Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), <https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html> (last visited Jan. 3, 2024).

⁵⁷ <https://integrisok.com/notice-of-privacy-practices>; <https://integrisok.com/landing/cyber-event>.

healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (Personal Information)” so that these companies can take the necessary precautions to thwart such attacks.⁵⁸

88. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a \$50 street value on the black market.⁵⁹

89. Integris’s assurances of maintaining high standards of cybersecurity make it evident that Integris recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained.

90. Integris was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

E. Integris Could Have Prevented the Data Breach.

91. Data breaches are preventable.⁶⁰ As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, “In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.”⁶¹ She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not

⁵⁸ Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014, <http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820> (last visited Jan. 3, 2024).

⁵⁹ *Study: Few Aware of Medical Identity Theft Risk*, Claims Journal (June 14, 2012), <https://www.claimsjournal.com/news/national/2012/06/14/208510.htm> (last visited Jan. 3, 2024).

⁶⁰ Lucy L. Thomson, “Despite the Alarming Trends, Data Breaches Are Preventable,” in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at <https://lawcat.berkeley.edu/record/394088>.

⁶¹ *Id.* at 17.

compromised”⁶²

92. “Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.”⁶³

93. In a Data Breach like this, many failures laid the groundwork for the Breach.

94. The FTC has published guidelines that establish reasonable data security practices for businesses.

95. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.⁶⁴

96. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.

97. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

⁶² *Id.* at 28.

⁶³ *Id.*

⁶⁴ *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

98. According to information and belief, Integris failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines.

99. Upon information and belief, Integris also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

100. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."⁶⁵

101. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider

⁶⁵ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.

using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁶⁶

102. Further, to prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and

⁶⁶ *Id.* at 3–4.

operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization’s helpdesk, search the internet for the sender organization’s website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website’s security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email’s legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....⁶⁷

103. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted from the Data Breach, Defendant could and should have implemented, as

⁶⁷ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at <https://www.cisa.gov/news-events/news/protecting-against-ransomware>.

recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
 - Apply latest security updates
 - Use threat and vulnerability management
 - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
 - Prioritize and treat commodity malware infections as potential full compromise
- **Include IT Pros in security discussions**
 - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely
- **Build credential hygiene**
 - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
 - Monitor for adversarial activities
 - Hunt for brute force attempts
 - Monitor for cleanup of Event Logs
 - Analyze logon events
- **Harden infrastructure**
 - Use Windows Defender Firewall
 - Enable tamper protection
 - Enable cloud-delivered protection
 - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].⁶⁸

104. Given that Defendant was storing the PII of millions of individuals, Defendant

⁶⁸ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

could have and should have implemented all of the above measures to prevent and detect cyberattacks.

105. Specifically, among other failures, Integris had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.⁶⁹

106. Moreover, it is a well-established industry standard practice for a business to dispose of confidential PII once it is no longer needed.

107. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: “Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it’s not on your system, it can’t be stolen by hackers.”⁷⁰ Integris, rather than following this basic standard of care, kept thousands of individuals’ unencrypted PII indefinitely.

108. In sum, the Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all PII.

109. Further, the scope of the Data Breach could have been dramatically reduced had Integris utilized proper record retention and destruction practices.

F. Plaintiffs’ Individual Experience

110. Plaintiffs are both clients of Defendant. Plaintiffs entrusted their PII to Defendant to receive medical services with the reasonable expectation and mutual understanding that

⁶⁹ See, e.g., <https://www.digitalguardian.com/blog/how-safeguard-your-business-data-encryption> (last visited Jan. 3, 2024).

⁷⁰ *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

Defendant would keep their PII secure from unauthorized access. By accepting Plaintiffs' PII, Defendant agreed to safeguard it and protect it from unauthorized access and delete it after a reasonable time.

111. Defendant was in possession of Plaintiffs' PII before, during, and after the Data Breach.

112. On December 27, 2023, Plaintiffs received an email from cybercriminals.⁷¹

113. The email from cybercriminals informed Plaintiffs that M.J.'s and over 2 million other patients' Social Security numbers, dates of birth, addresses, phone numbers, insurance information, and employer information was accessed in a massive data breach against Integris, perpetrated by the cybercriminals.⁷²

114. The cybercriminals confirmed it stole M.J.'s PII in the Data Breach in the email it sent to Plaintiffs, which contained M.J.'s name, date of birth, address, and Social Security number.⁷³

115. The email threatened Plaintiffs that if they did not pay the extortion demand of \$50.00 before January 5, 2024, M.J.'s data would be sold to data brokers on the dark web.⁷⁴

116. Cybercriminals provided a dark web website link for Plaintiffs to purchase M.J.'s data from them.⁷⁵

117. According to the cybercriminals, its "tor shop allows users to purchase data for fraud. Any buyer can purchase data 'exclusively' for 50\$. This gives the buyer exclusive rights on

⁷¹ See Exhibit 1.

⁷² *Id.*

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *Id.*

the data and will remove the data from the shop completely. This feature is useful for fraud activity such as identity theft, opening SIM lines, opening bank accounts, taking out loans, and making USA companies. A buyer can also purchase data without exclusive rights for 3\$. In this case, the data will still be listed on the shop.”⁷⁶

118. After receiving this threatening and highly disturbing email from cybercriminals, Plaintiffs have experienced severe anxiety and emotional distress.

119. As a direct and traceable result of the Data Breach, Plaintiffs have been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which includes researching the Data Breach, reviewing, and monitoring their accounts for fraudulent activity, reviewing his credit reports, placing a freeze on his credit, and researching credit monitoring services.

120. Plaintiffs will be forced to expend additional time to review their credit reports and monitor their accounts for the rest of their lives.

121. Plaintiffs place significant value in the security of their PII and do not readily disclose it. Plaintiffs entrusted their PII to Defendant with the understanding that Defendant would keep this information secure and would employ reasonable and adequate security measures to ensure that their PII would not be compromised.

122. Plaintiffs have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

123. As a direct and traceable result of the Data Breach, Plaintiffs suffered actual damages such as: (1) lost time related to monitoring their accounts and credit reports for fraudulent activity; (2) loss of privacy due to M.J.’s PII being accessed by cybercriminals; (3) loss of the

⁷⁶ *Id.*

benefit of the bargain because Defendant did not adequately protect their PII; (4) emotional distress because identity thieves now possess M.J.'s first and last name paired with her Social Security number and other sensitive information; (5) exposure to increased and imminent risk of fraud and identity theft now that M.J.'s PII has been accessed and misused; (6) the loss in value of their PII due to M.J.'s PII being in the hands of cybercriminals who can use it at their leisure; (7) actual misuse of M.J.'s PII; and (8) other economic and noneconomic harm.

124. Plaintiffs have been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for *years* to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach and the fact that the cybercriminals had already threatened misuse of PII.⁷⁷

125. Knowing that thieves intentionally targeted and stole M.J.'s PII, including her Social Security number, and knowing that her PII is in the hands of cybercriminals has caused great anxiety beyond mere worry. Specifically, Plaintiff, Teresa Johnston, has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that M.J.'s PII has been stolen.

126. Plaintiffs have a continuing interest in ensuring that M.J.'s PII, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs', and the Class's PII will be wholly unprotected and at-risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

127. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

128. Plaintiffs bring this action against Integris on behalf of themselves and all other

⁷⁷ *Id.*

individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of a nationwide class (the “Class”) defined as follows:

All persons whose PII was compromised in the Integris Data Breach occurring in or around November 2023.

129. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant’s officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

130. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

131. Plaintiffs anticipate the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant’s own business records or electronic media can be utilized for the notice process.

132. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

133. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. The total number of individuals affected is more than two million.

134. **Typicality:** Plaintiffs’ claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Integris’s uniform misconduct. Integris’s inadequate data security gave rise to Plaintiffs’ claims and are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Integris.

135. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs’ interests do not conflict with the interests of the Class; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs’ counsel

intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

136. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Integris's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

137. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- a. Whether Defendant engaged in the wrongful conduct alleged herein;
- b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PII;
- c. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;
- d. Whether Integris breached its duties to Plaintiffs and the Class;
- e. Whether Integris failed to provide adequate cyber security;
- f. Whether Integris knew or should have known that its computer and network

security systems were vulnerable to cyber-attacks;

- g. Whether Integris's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;
- h. Whether Integris was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;
- i. Whether Integris breached implied contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PII;
- j. Whether Integris failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;
- k. Whether Integris continues to breach duties to Plaintiffs and the Class;
- l. Whether Plaintiffs and the Class suffered injury as a proximate result of Integris's negligent actions or failures to act;
- m. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and
- n. Whether Integris's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION NEGLIGENCE

(On Behalf of Plaintiffs and the Class)

138. Plaintiffs incorporate foregoing paragraphs as though fully set forth herein.

139. Integris solicited, gathered, and stored the PII of Plaintiffs and Class Members.

140. Upon accepting and storing the PII of M.J. and Class members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of M.J. and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

141. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class members could and would suffer if the PII was wrongfully disclosed. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

142. Because of this special relationship, Defendant required Plaintiffs and Class members to provide their PII, including names, Social Security numbers, and other PII.

143. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class members in its possession was only used for the provided purpose and that Defendant would destroy any PII that it was not required to maintain.

144. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

145. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiffs' and Class members' PII from being foreseeably accessed, and its improper retention of PII it was not required to maintain, Defendant negligently failed to observe and perform its duty.

146. Plaintiffs and Class members did not receive the benefit of the bargain with Defendant, because providing their PII was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

147. Defendant was aware of the fact that cybercriminals routinely target healthcare entities through cyberattacks in an attempt to steal patient and employee PII. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement

reasonable security measures.

148. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiffs and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

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

150. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiffs and the Class include:

- a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' PII was adequately secured from impermissible release, disclosure, and publication;
- b. To protect Plaintiffs' and Class members' PII in its possession by using reasonable and adequate security procedures and systems;
- c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and
- d. To promptly notify Plaintiffs and Class members of any data breach, security incident, or intrusion that affected or may have affected their PII.

151. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties,

creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

152. Plaintiffs' injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

153. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class members' PII. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the PII in its possession;
- b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;
- c. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's PII;
- d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;
- e. Failing to promptly notify Plaintiffs and Class members of the Data Breach that affected their PII.

154. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

155. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

156. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class members while it was within Defendant's possession and

control.

157. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class members, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps to secure their PII and mitigate damages.

158. Plaintiffs and Class members could have taken actions earlier had they been timely notified of the Data Breach.

159. Plaintiffs and Class members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

160. Plaintiffs and Class members have suffered harm from the delay in notifying them of the Data Breach.

161. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiffs and Class members have suffered, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and

non-economic losses; (vii) the continued risk to their PII, 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 the PII of patients in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

162. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

163. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

**SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)**

164. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

165. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and the Class.

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

167. Defendant gathered and stored the PII of Plaintiffs and the Class as part of its business which affects commerce.

168. Defendant violated the FTC Act by failing to use reasonable measures to protect

the PII of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

169. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class members' PII, and by failing to provide prompt notice without reasonable delay.

170. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

171. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

172. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

173. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII.

174. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

175. Defendant's violations of the FTC Act constitute negligence *per se*.

176. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

177. The injury and harm that Plaintiffs and Class members suffered (as alleged above)

was the direct and proximate result of Defendant's negligence *per se*.

178. Plaintiffs and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

**THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)**

179. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

180. Defendant acquired and maintained the PII of Plaintiffs and the Class including their Social Security numbers and other sensitive information.

181. Plaintiffs and Class Members reasonably expected that their PII that they entrusted to Integris would remain confidential and would not be shared or disclosed to criminal third parties.

182. Plaintiffs and Defendant had an understanding that Defendant would take steps to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect their sensitive PII and Plaintiffs and Defendant had an expectation that Defendant would not share or disclose, whether intentionally or unintentionally, sensitive PII in the absence of authorization for any purpose.

183. Defendant entered into implied contracts with Plaintiffs and the Class in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII and timely notify them of a data breach.

184. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and the Class Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

185. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach.

186. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' PII.

187. Plaintiffs and the Class have suffered injuries as described herein, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

**FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)**

188. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

189. Plaintiffs allege this claim in the alternative to their breach of implied contract claim.

190. Plaintiffs and the Class provided their PII to Integris.

191. By conferring their PII to Defendant, Plaintiffs and the Class reasonably understood Defendant would be responsible for securing their PII in Defendant's possession.

192. Through the collection and use of Plaintiffs' and the Class's PII, Defendant was able to provide medical services, and able to run its business and receive substantial revenue it otherwise would not have been able to receive.

193. Defendant collected, maintained, and stored the PII of Plaintiffs and the Class, and as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiffs and the Class.

194. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

195. However, acceptance of the benefit under the facts and circumstances outlined

above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

196. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

197. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

198. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have allowed Defendant to collect their PII.

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

200. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine for themselves how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the 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; (vi) the continued risk to their PII, 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 PII in their continued possession; and/or (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

202. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, all gains that it unjustly received.

**FIFTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)**

203. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

204. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

205. As previously alleged, Plaintiffs and members of the Class entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the PII collected from Plaintiffs and the Class.

206. Defendant owed and still owes a duty of care to Plaintiffs and Class members that require it to adequately secure Plaintiffs' and Class members' PII.

207. Upon reason and belief, Defendant still possesses the PII of Plaintiffs and the Class members.

208. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class members.

209. Since the Data Breach, Defendant has not yet announced any 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 go undetected and, thereby, prevent further attacks.

210. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

211. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

212. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

213. Plaintiffs and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

- a. Ordering that Defendant engage 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;

- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
- d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;
- e. Ordering that Defendant conduct regular database scanning and security checks; and
- f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

- a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;
- b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, prejudgment and post-judgment interest, attorney fees, expenses, and costs, as allowable by law;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;
- e. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: January 19, 2024

Respectfully submitted,

/s/ Larry D. Lahman

Larry D. Lahman, OBA No. 5166
Roger L. Ediger, OBA No. 19449
MITCHELL DECLERCK
202 West Broadway Avenue
Enid, OK 73701
Telephone: (580) 234-5144
Fax: (580) 234-8890
Email: ldl@mdpllc.com
Email: rle@mdpllc.com

Roberta D. Liebenberg*
Gerard A. Dever*
Jessica D. Khan*
FINE, KAPLAN AND BLACK, R.P.C.
One South Broad Street, 23rd Floor
Philadelphia, PA 19107
Telephone: (215) 567-6565
Email: rliebenberg@finekaplan.com

Michael E. Criden*
Lindsey C. Grossman*
CRIDEN & LOVE, P.A.
7301 SW 57th Court, Suite 515
South Miami, Florida 33143
Telephone: 305-357-9000
Fax: 305-357-9050
Email: mcriden@cridenlove.com
Email: lgrossman@cridenlove.com

** Pro Hac Vice Application Forthcoming*

*Attorneys for Plaintiff and the
Proposed Class*

Exhibit 1 - Email

From: **Administrator** <Administrator@depestino.perfectsoccerskills.com>

Date: Sun, Dec 24, 2023, 1:26 PM

Subject: [INTEGRISOK BREACH] Your personal data is selling on the darknet

To: <johnstonspatch6@gmail.com>

Integris Health ([integrisok.com](https://www.integrisok.com)) was breached on November 2023. The data of over 2 million patients was compromised including SSN, DOB, Address, Phone, Insurance Information, and Employer Information. This data will sell on the darknet and be used for fraud and identity theft. If you are receiving this message, your data have been compromised. We provide a sample of your data as proof.

OKLAHOMA CITY OK

[405-888-6957](tel:405-888-6957),

2016

We have contacted Integris Health, but they refuse to resolve this issue. We give you the opportunity to remove your personal data from our databases before we sell the entire database to data brokers on Jan 5 2024.

Our tor shop allows users to purchase data for fraud. Any buyer can purchase data "exclusively" for 50\$. This gives the buyer exclusive rights on the data and will remove the data from the shop completely. This feature is useful for fraud activity such as identity theft, opening SIM lines, opening bank accounts, taking out loans, and making USA companies. A buyer can also purchase data without exclusive rights for 3\$. In this case, the data will still be listed on the shop.

You can remove your data from our shop and protect it from future fraud by purchasing exclusive rights on it (50\$).

Instructions to access our shop:

- 1) Download and install Tor Browser from: <https://torproject.org/>
- 2) Navigate to: <http://3z3si7qa7e6uujcft7j5mmns4p3cy7dmmggkqfo7bssvbrh4v56j6byd.onion/register>
- 3) Create an account and login
- 4) Purchase credits with BTC (<https://coinbase.com> <https://binance.com>)
- 5) Find your data and click "REMOVE"

If you purchase the 50\$, and you are unhappy about this data, contact our support at data.seller@onionmail.org and we will refund you 45\$ then add the data back to the shop and it will show +1 for Buys. We keep 5\$ because you still view the data.

If you have questions or problems, contact data.seller@onionmail.org

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

<p>I. (a) PLAINTIFFS TERESA JOHNSTON, indiv & as parent & natural guardian of M.J., a minor, & on behalf of all others similarly situated,</p> <p>(b) County of Residence of First Listed Plaintiff <u>Oklahoma</u> (EXCEPT IN U.S. PLAINTIFF CASES)</p> <p>(c) Attorneys (Firm Name, Address, and Telephone Number) Larry D. Lahman and Roger L. Ediger MITCHELL DeCLERCK, 202 West Broadway, Enid, OK 73701 (580) 234-5144</p>	<p>DEFENDANTS INTEGRIS HEALTH, INC.</p> <p>County of Residence of First Listed Defendant <u>Oklahoma</u> (IN U.S. PLAINTIFF CASES ONLY)</p> <p>NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.</p> <p>Attorneys (If Known)</p>
--	---

<p>II. BASIS OF JURISDICTION (Place an "X" in One Box Only)</p> <p><input type="checkbox"/> 1 U.S. Government Plaintiff</p> <p><input checked="" type="checkbox"/> 3 Federal Question (U.S. Government Not a Party)</p> <p><input type="checkbox"/> 2 U.S. Government Defendant</p> <p><input type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III)</p>	<p>III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)</p> <table border="1" style="width:100%; border-collapse: collapse;"> <tr> <td></td> <td>PTF</td> <td>DEF</td> <td></td> <td>PTF</td> <td>DEF</td> </tr> <tr> <td>Citizen of This State</td> <td><input checked="" type="checkbox"/> 1</td> <td><input type="checkbox"/> 1</td> <td>Incorporated or Principal Place of Business In This State</td> <td><input type="checkbox"/> 4</td> <td><input checked="" type="checkbox"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td><input type="checkbox"/> 2</td> <td><input type="checkbox"/> 2</td> <td>Incorporated and Principal Place of Business In Another State</td> <td><input type="checkbox"/> 5</td> <td><input type="checkbox"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td><input type="checkbox"/> 3</td> <td><input type="checkbox"/> 3</td> <td>Foreign Nation</td> <td><input type="checkbox"/> 6</td> <td><input type="checkbox"/> 6</td> </tr> </table>		PTF	DEF		PTF	DEF	Citizen of This State	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4	Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5	Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6
	PTF	DEF		PTF	DEF																				
Citizen of This State	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4																				
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5																				
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6																				

IV. NATURE OF SUIT (Place an "X" in One Box Only) Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<p>PERSONAL INJURY</p> <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input checked="" type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<p>PERSONAL INJURY</p> <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability <p>PERSONAL PROPERTY</p> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Injury Product Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <p>PROPERTY RIGHTS</p> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <p>SOCIAL SECURITY</p> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g))	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	LABOR	FEDERAL TAX SUITS	
<input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	<p>Habeas Corpus:</p> <input type="checkbox"/> 510 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <p>Other:</p> <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement	<input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act	<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	

V. ORIGIN (Place an "X" in One Box Only)

1 Original Proceeding
 2 Removed from State Court
 3 Remanded from Appellate Court
 4 Reinstated or Reopened
 5 Transferred from Another District (specify)
 6 Multidistrict Litigation - Transfer
 8 Multidistrict Litigation - Direct File

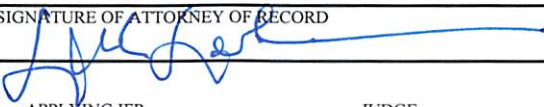
VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
 Class Action Fairness Act (CAFA), 28 U.S.C. 1322(d), 28 U.S.C. 1391(a)(1)

Brief description of cause:
 Data Breach Clas Action

VII. REQUESTED IN COMPLAINT:
 CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.
DEMAND \$ 5,000,000.00
 CHECK YES only if demanded in complaint: **JURY DEMAND:** Yes No

VIII. RELATED CASE(S) IF ANY (See instructions):
 JUDGE see attached sheet
 DOCKET NUMBER _____

DATE: 01/19/2024
 SIGNATURE OF ATTORNEY OF RECORD: 

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

The following related cases are pending in the Western District of Oklahoma (“Related Cases”):

1. ***Johnson et al v. Integris Health Inc.***, 5:23-cv-01192-D filed 12/27/2023,
2. ***Roof v. Integris Health Inc.***, 5:23-cv-01200-D filed 12/28/2023,
3. ***Bointy et al v. Integris Health Inc.***, 5:23-cv-01206-D filed 12/29/2023,
4. ***Leeb et al v. Integris Health Inc.***, 5:23-cv-01207-D filed 12/29/2023,
5. ***Zinck et al v. Integris Health Inc.***, 5:23-cv-01208-D filed 12/29/2023,
6. ***Campbell-Detrixhe et al v. Integris Health Inc.***, 5:23-cv-01209-D filed 12/29/2023,
7. ***Civi et al v. Integris Health Inc.***, 5:23-cv-01210-D filed 12/29/2023,
8. ***DiCenso et al v. Integris Health Inc.***, 5:24-cv-00011-D filed 01/03/2024,
9. ***Owens et al v. Integris Health Inc.***, 5:24-cv-00020-D filed 01/08/2024; and
10. ***King et al v. Integris Health Inc.***, 5:24-cv-00022-D filed 01/08/2024

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
 United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.