UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

AARON ZINCK, on behalf of himself and on behalf of all others similarly situated,

Plaintiff,

v.

INTEGRIS HEALTH, INC.,

Defendant.

Case No. CIV-23-1208-J

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Aaron Zinck ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through his undersigned counsel, and files this Class Action Complaint against Integris Health, Inc. ("Integris" or "Defendant") and alleges the following based on personal knowledge of facts, upon information and belief, and based on the investigation of his counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Integris for its negligent failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII") culminating in a massive and preventable data breach (the "Data Breach" or "Breach"). As a result of Integris's insufficient data security, cybercriminals easily infiltrated Integris's inadequately protected computer systems and

stole the PII of Plaintiff 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 Plaintiff'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.

2. On or around December 24, 2023, through December 27, 2023, victims of the Data Breach (including Plaintiff and Class Members) began receiving emails from cybercriminal "DataLeakege@consultas.itev.com.br" (referred to herein as "DataLeakege"), cautioning Plaintiffs and Class Members that Integris was breached in November 2023, impacting over 2 million patients.

3. DataLeakege explicitly stated to Plaintiff and Class Members in the email, "[i]f you are receiving this message, your data have [sic] been compromised."[1]

4. In this email, DataLeakege admitted highly sensitive information such as "SSN, DOB, Address, Phone, Insurance Information, and Employer Information" were compromised in the Data Breach.[2]

5. DataLeakege also threatened Plaintiff and Class Members that their "data will sell [sic] on the darknet and be used for fraud and identity theft."[3]

6. What is perhaps most disturbing, however, is that in the email, DataLeakege provided Plaintiff's address, telephone number, date of birth, and Social Security number as proof that it had indeed stolen Plaintiff's PII from Integris.[4]

---

[1] *Id.*
[2] *Id.*
[3] *Id.*
[4] *Id.*

7. DataLeakege then extorted Plaintiff and the Class by giving them until before 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.[5] If Plaintiff and the Class failed to do so, DataLeakege threatened it would sell the entire database to data brokers on January 5, 2024.[6]

8. According to DataLeakege's 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$)."[7]

9. The email then gave instructions on how to access the information stolen in the Data Breach on the dark web, thus Plaintiff's and the Class's PII is available for anyone to access and view.[8]

10. According to DataLeakege, it contacted Integris after the Breach, but Integris "refused to resolve this issue."[9]

---

[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*

11. This disturbing email from DataLeakege makes it clear that Plaintiff and the Class are at an imminent risk of fraud and identity theft.

12. It was not until Plaintiff and the Class were being extorted by DataLeakege that Integris made a public statement regarding the Data Breach.[10]

13. On December 24, 2023, Integris publicly announced it experienced a data breach on its website.[11]

14. According to Integris, on an undisclosed date, Integris discovered unauthorized activity on certain systems.[12]

15. After becoming aware of the suspicious activity, Integris initiated an investigation into the nature and scope of the activity.[13]

16. Integris claims that the investigation determined that certain files may have been accessed by an unauthorized party on November 28, 2023.[14]

17. However, on December 24, 2023, Integris learned that patients began receiving communications from a group claiming responsibility for the unauthorized access.[15]

[10] *Id.*
[11] https://integrisok.com/landing/cyber-event.
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*

18. 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.[16] But Integris offered no assurance it would retrieve the stolen information.

19. 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.

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

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

22. 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.

23. Now, for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a

[16] *Id.*

direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, loss of privacy, and/or additional damages as described below.

24. Plaintiff brings this action individually and on behalf of the Class, seeking 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

25. Plaintiff **Aaron Zinck** is an individual domiciled in Dell City, Oklahoma. On or about December 27, 2023, Plaintiff received the email from DataLeakege, notifying him that his name, address, date of birth, and Social Security number, were stolen in the Data Breach and were available for purchase on the dark web.

26. 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

27. 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.

28. This Court has personal jurisdiction over Defendant because Defendant is incorporated and/or has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

29. 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 Plaintiff's and the Class's PII.

30. Integris Health is Oklahoma's largest not-for-profit health network, operating hospitals, clinics, and urgent care throughout the state.[17]

31. Integris employs more than 9,000 people and generates approximately $1.5 billion in annual revenue.[18] These statistics make it apparent Integris could have afforded to implement adequate data security prior to the Breach but deliberately chose not to.

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

---

[17] *See* https://www.bleepingcomputer.com/news/security/integris-health-patients-get-extortion-emails-after-cyberattack/.

[18] https://www.zippia.com/integris-health-careers-27390/revenue/.

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

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

35. Integris recognizes this duty to protect and safeguard Plaintiff's 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."[19]

36. However, Integris failed to protect Plaintiff's and the Class's PII.

37. As a result, Plaintiff's 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 threat actor themselves—DataLeakege.

B. Integris's Massive and Preventable Data Breach.

38. In or around late December 2023, extortion emails were sent to Plaintiff and the Class by a cybercriminal group under the name of "DataLeakege," who claimed it stole the PII of over 2 million patients in a cyberattack against Integris in November 2023.[20]

[19] https://integrisok.com/landing/cyber-event.
[20] *Id.*; https://www.bleepingcomputer.com/news/security/integris-health-patients-get-extortion-emails-after-cyberattack/

39. DataLeakege claims 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.[21] It is also apparent it stole the email addresses of Plaintiff and the Class.[22]

40. DataLeakege explicitly informed Plaintiff and the Class in its extortion email that "[i]f you are receiving this message, your data have [sic] been compromised."[23]

41. DataLeakege also provided a sample of the victim's stolen data as proof to confirm DataLeakege had accessed and stolen the victim's name, address, phone number, date of birth, and Social Security in the Breach.[24]

42. Further, DataLeakege 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$).

43. 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,

[21] *See* Exhibit 1.
[22] *Id.*
[23] *Id.*
[24] *Id.*

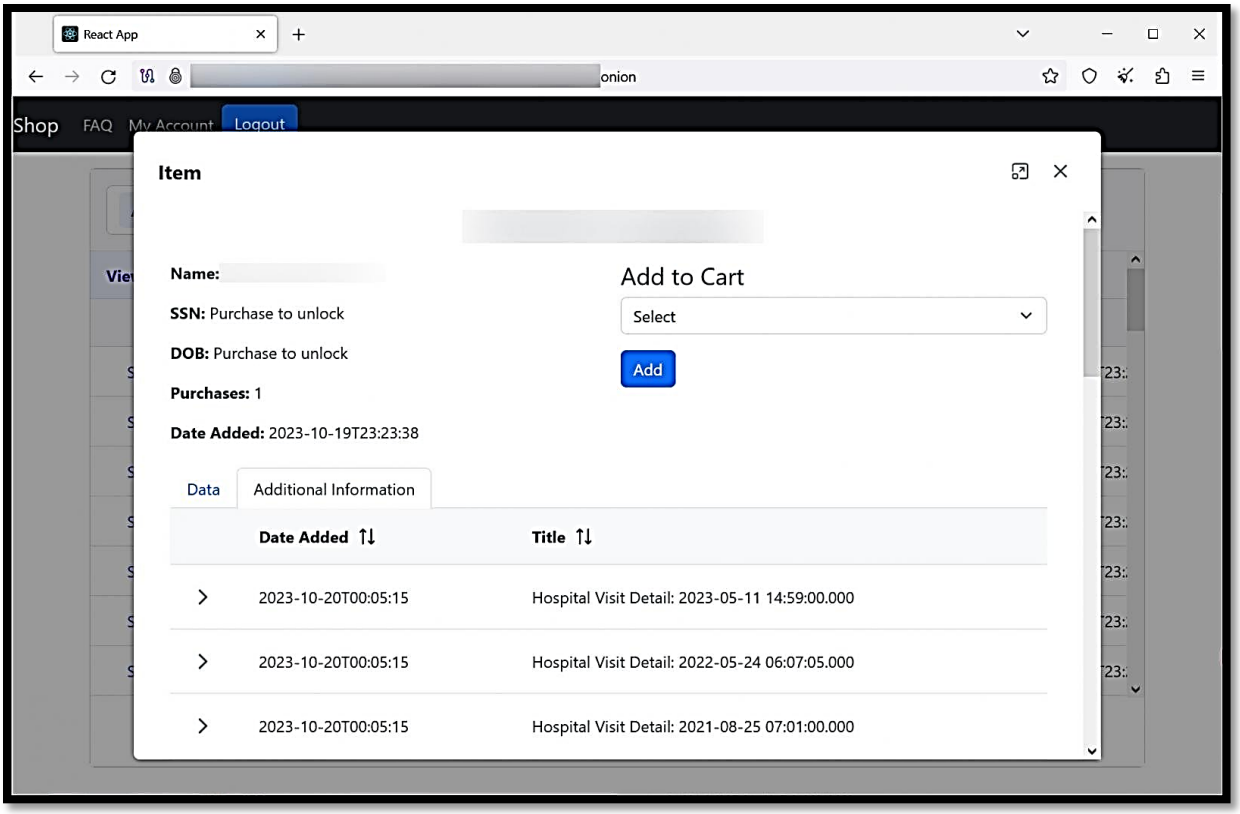
Social Security Numbers, dates of birth, and information about hospital visits.[25]

44. 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.[26] Signaling that this was a financially motivated Breach that potentially spanned months.

45. Below is a screenshot of the Tor dark web site selling the PII stolen in the Data Breach:[27]

[IMAGE ON NEXT PAGE]

[25] https://www.bleepingcomputer.com/news/security/integris-health-patients-get-extortion-emails-after-cyberattack/
[26] https://www.bleepingcomputer.com/news/security/integris-health-patients-get-extortion-emails-after-cyberattack/
[27] *Id.*



46. As threat actors can use the exposed data to conduct identity theft, some patients may be tempted to pay to delete the data.[28] However, as previous extortion demands have shown, paying a ransom does not always lead to the actual deletion of data.[29]

47. It was only after DataLeakege started extorting Data Breach victims did Integris publicly announce the Data Breach.

48. Integris Health uploaded a notice to its website on December 24, 2023, finally informing the public of the Data Breach.[30]

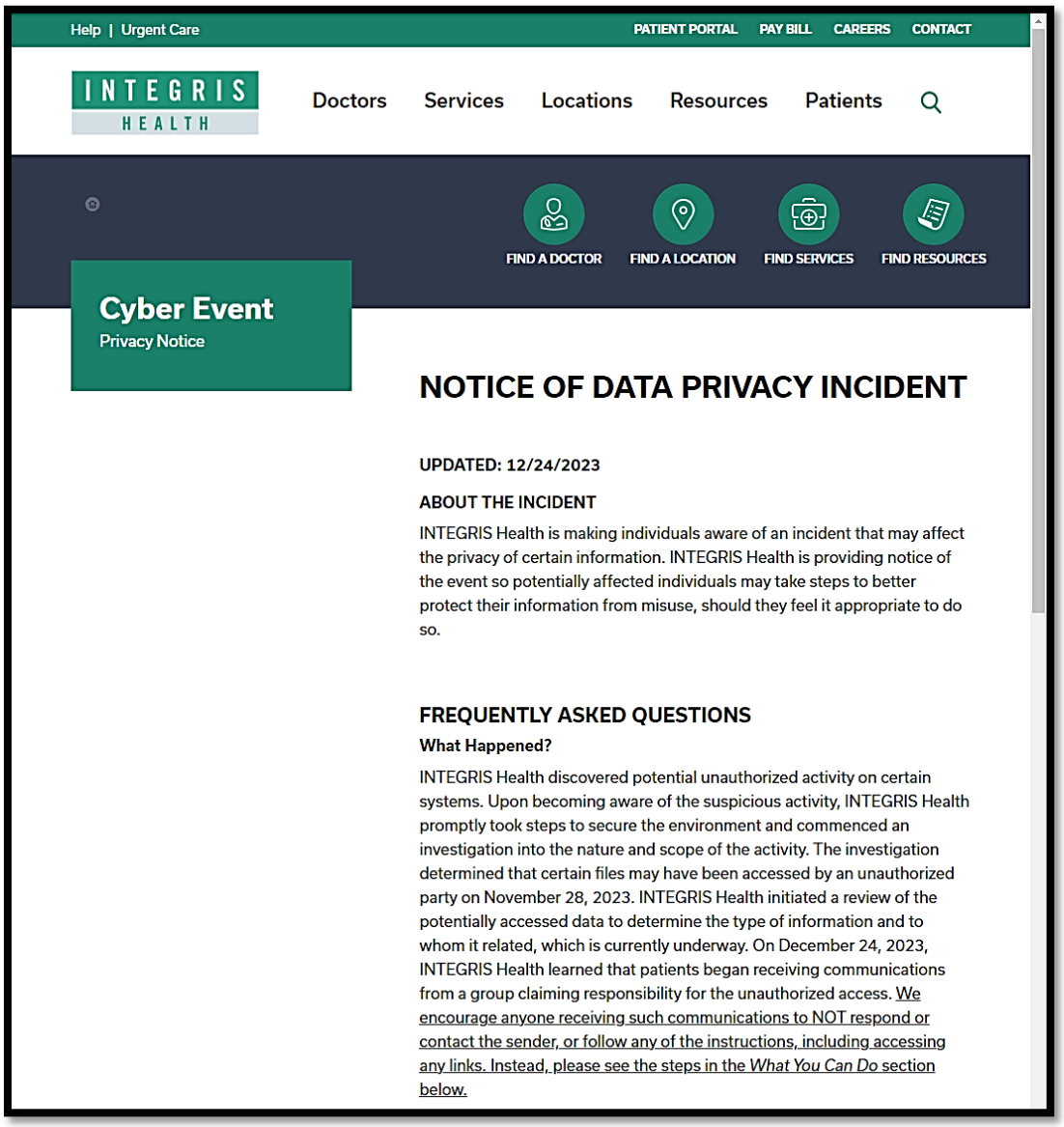
---

[28] *Id.*

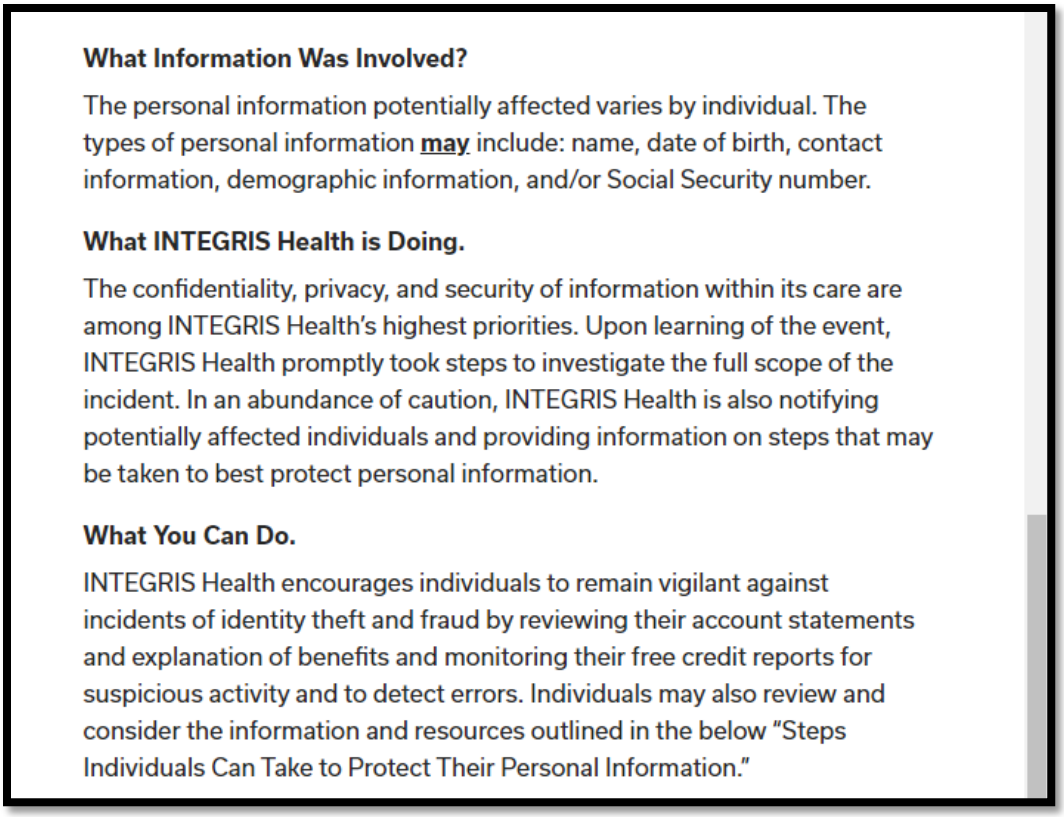
[29] https://www.bleepingcomputer.com/news/security/scam-psa-ransomware-gangs-dont-always-delete-stolen-data-when-paid/.

[30] https://www.hipaajournal.com/integris-health-data-breach/; https://integrisok.com/landing/cyber-event.

49. The images below show portions of the notice that appears on Integris's website:[31]



[31] *Id.*



What Information Was Involved?

The personal information potentially affected varies by individual. The types of personal information **may** include: name, date of birth, contact information, demographic information, and/or Social Security number.

What INTEGRIS Health is Doing.

The confidentiality, privacy, and security of information within its care are among INTEGRIS Health's highest priorities. Upon learning of the event, INTEGRIS Health promptly took steps to investigate the full scope of the incident. In an abundance of caution, INTEGRIS Health is also notifying potentially affected individuals and providing information on steps that may be taken to best protect personal information.

What You Can Do.

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

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

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

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

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

54. 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 Plaintiff and the Class Members and to profit off their misfortune.

55. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[32]

56. 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 other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[33] **Indeed, DataLeakege highlights in its email how Plaintiff's and the Class's PII can be misused.**[34] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

57. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

---

[32] *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 Oct. 9, 2023).

[33] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Oct. 9, 2023).

[34] Exhibit 1.

> **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.[35]
>
> (Emphasis added.)

58. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[36]

59. 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 in the kinds of criminal activity described herein. Indeed, DataLeakege's email admits as much.[37]

60. A social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[38]

---

[35] *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 Oct. 9, 2023).

[36] *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.

[37] *See* Exhibit 1.

[38] 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 Oct. 9, 2023).

61. "[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."[39]

62. 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***.[40]

63. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

64. 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.[42]

---

[39] *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 Oct. 9, 2023).

[40] 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 Oct. 9, 2023).

[41] *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.

[42] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Oct. 9, 2023).

65. 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.

66. 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.[43]

67. Defendant's made no offer of identity monitoring to Plaintiff 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 Plaintiff from the damages and harm caused by its failures.

68. 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.

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

70. 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

[43] *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.

another person's PII)—it does not prevent identity theft.[44] Nor can an identity monitoring service remove personal information from the dark web.[45]

71. "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."[46]

72. As a direct and proximate result of the Data Breach Plaintiff 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. Plaintiff and the Class must now take the time and 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.

73. Even more seriously is the identity restoration that Plaintiff 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

[44] *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 Oct. 9, 2023).
[45] *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 Oct. 9, 2023).
[46] *Id.*

cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

74. Plaintiff and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property including PII;

c. Improper disclosure of their PII;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their PII;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breaches;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

75. Moreover, Plaintiff 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 Plaintiff's PII.

76. Plaintiff 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.

77. 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."[47]

78. At Integris's suggestion, Plaintiff is desperately trying to mitigate the damage that Integris has caused him.

79. Given the kind of PII Integris made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because identity thieves have his PII, Plaintiff and

[47] https://integrisok.com/landing/cyber-event.

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.[48]

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

D. Defendant was Aware of the Risk of Cyberattacks.

81. 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,[49] Yahoo,[50] Marriott International,[51] Chipotle, Chili's, Arby's,[52] and others.[53]

---

[48] *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 Oct. 9, 2023).

[49] 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 Oct. 9, 2023).

[50] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last visited Oct. 9, 2023).

[51] 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 visited Oct. 9, 2023).

[52] 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/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (last visited Oct. 9, 2023).

[53] *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/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited Oct. 9, 2023).

82. Integris should certainly have been aware, and indeed was aware,[54] 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.

83. 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.

84. 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 Breaches.

85. Data breaches are preventable.[55] 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."[56] 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 compromised . . . ."[57]

86. "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

[54] https://integrisok.com/notice-of-privacy-practices;https://integrisok.com/landing/cyber-event.
[55] 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.
[56] *Id.* at 17.
[57] *Id.* at 28.

information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[58]

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

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

89. 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.[59]

90. 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.

91. 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.

---

[58] *Id.*

[59] *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.

92. 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.

93. 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.

94. 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."[60]

95. 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.

[60] *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.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[61]

96. Further, to prevent and detect malware attacks, including the malware attacks that resulted in the Data Breach, Defendant could and should have implemented,

[61] *Id.* at 3–4.

as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and 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….[62]

97. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
    - Apply latest security updates
    - Use threat and vulnerability management

[62] *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.

- 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].[63]

98. Given that Defendant was storing the PII of millions of individuals, Defendant could have and should have implemented all of the above measures to prevent and detect cyberattacks.

99. 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.[64]

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

101. 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."[65] Integris, rather than

---

[63] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[64] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption (last visited Oct. 9, 2023).

[65] *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.

following this basic standard of care, kept thousands of individuals' unencrypted PII indefinitely.

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

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

F. Plaintiff's Individual Experience

104. Plaintiff is a former patient of Defendant. Plaintiff entrusted his PII to Defendant to receive medical services with the reasonable expectation and mutual understanding that Defendant would keep his PII secure from unauthorized access. By accepting Plaintiff's PII, Defendant agreed to safeguard it and protect it from unauthorized access and delete it after a reasonable time.

105. Defendant was in possession of Plaintiff's PII before, during, and after the Data Breach.

106. In or around December 2023, Plaintiff received an email from DataLeakege@consultas.itev.com.br.[66]

107. The email from DataLeakege informed Plaintiff that his 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 DataLeakege.[67]

[66] *See* Exhibit 1.
[67] *Id.*

108. DataLeakege confirmed it stole Plaintiff's PII in the Data Breach in the email it sent to Plaintiff, which contained his name, date of birth, address, and Social Security number.[68]

109. The email threatened Plaintiff that if he did not pay the extortion demand of $50.00 before January 5, 2024, his data would be sold to data brokers on the dark web.[69]

110. DataLeakege provided a dark web website link for Plaintiff to purchase his data from DataLeakege.[70]

111. According to DataLeakege, 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."[71]

112. As a direct and traceable result of the Data Breach, Plaintiff has 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 his accounts for fraudulent activity, reviewing his credit reports, placing a freeze on his credit, and researching credit monitoring services. In total, Plaintiff estimates he has already spent eight (8) hours responding to the Data Breach. However, this is not the end. Plaintiff will

[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*

be forced to expend additional time to review his credit reports and monitor his accounts for the rest of his life. This is time spent at Defendant's direction, which has been lost forever and cannot be recaptured.

113. Additionally, on November 22, 2023, Plaintiff received a notification informing him of fraudulent Cash App charges to his USAA bank account from someone who had obtained his debit card information. As a result, Plaintiff was forced to spend the time and effort obtaining a new debit card. Plaintiff reasonably believes this instance of fraud is fairly traceable to the Data Breach due to DataLeakege's email and the proximity of the transaction to the Breach.

114. Plaintiff places significant value in the security of his PII and does not readily disclose it. Plaintiff entrusted his PII to Defendant with the understanding that Defendant would keep this information secure and would employ reasonable and adequate security measures to ensure that his PII would not be compromised.

115. Plaintiff has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

116. As a direct and traceable result of the Data Breach, Plaintiff suffered actual damages such as: (1) lost time related to monitoring his accounts and credit reports for fraudulent activity; (2) loss of privacy due to his PII being accessed by cybercriminals; (3) loss of the benefit of the bargain because Defendant did not adequately protect his PII; (4) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (5) exposure to increased and imminent risk of fraud and identity theft now that his PII has been accessed and misused;

(6) the loss in value of their PII due to his PII being in the hands of cybercriminals who can use it at their leisure; (7) actual misuse of his PII; and (8) other economic and non-economic harm.

117. Plaintiff has 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 DataLeakege has already threatened misuse of PII.[72]

118. Knowing that thieves intentionally targeted and stole his PII, including his Social Security number, and knowing that his PII is in the hands of cybercriminals has caused great anxiety beyond mere worry. Specifically, Plaintiff 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 his PII has been stolen.

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

V. CLASS ACTION ALLEGATIONS

120. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

[72] *Id.*

121. Plaintiff brings this action against Integris on behalf of himself and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts 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.**

122. 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.

123. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

124. Plaintiff anticipates 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.

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

126. **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.[73]

127. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Integris's uniform misconduct.

[73] *Id.*

Integris's inadequate data security gave rise to Plaintiff's claims and are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Integris.

128. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

129. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff 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.

130. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff 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 Plaintiff's and the Class's PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Integris breached its duties to Plaintiff 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 off vast numbers of individuals to be stored within its network;

i. Whether Integris was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breaches to include former employees and business associates;

j. Whether Integris breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their PII;

k. 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 Plaintiff and the Class;

l. Whether Integris continues to breach duties to Plaintiff and the Class;

m. Whether Plaintiff and the Class suffered injury as a proximate result of Integris's negligent actions or failures to act;

n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Integris's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

131. Plaintiff incorporates foregoing paragraphs as though fully set forth herein.

132. Integris solicited, gathered, and stored the PII of Plaintiff and Class Members.

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

134. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if the PII was wrongfully disclosed. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiff 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 Plaintiff and the Class.

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

136. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff 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.

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

138. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiff's 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.

139. Plaintiff 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.

140. 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.

141. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff 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 Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

142. Defendant's duty extended to protecting Plaintiff 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.

143. Defendant had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiff 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 Plaintiff's and Class members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's 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 Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their PII.

144. Plaintiff 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 Plaintiff and the Class had entrusted to it.

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

146. Defendant breached its duties of care by failing to adequately protect Plaintiff's 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 Plaintiff and the Class's PII;

d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

e. Failing to promptly notify Plaintiff and Class members of the Data Breaches that affected their PII.

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

148. 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, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

149. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiff 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 Plaintiff and Class members while it was within Defendant's possession and control.

150. Further, through its failure to provide timely and clear notification of the Data Breaches to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps to securing their PII and mitigating damages.

151. Plaintiff and Class members could have taken actions earlier had they been timely notified of the Data Breaches.

152. Plaintiff 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 Breaches more quickly.

153. Plaintiff and Class members have suffered harm from the delay in notifying them of the Data Breaches.

154. 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, Plaintiff and Class members have suffered, as Plaintiff have, 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 Breaches, 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 employees 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, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

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

156. Plaintiff 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 Plaintiff and the Class)

157. Plaintiff incorporates foregoing paragraphs as though fully set forth herein.

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

159. 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.

160. Defendant gathered and stored the PII of Plaintiff and the Class as part of their business which affects commerce.

161. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

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

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

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

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

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

167. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breaches expeditiously and/or as soon as practicable to Plaintiff and the Class.

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

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

170. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

171. Plaintiff 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 Plaintiff and the Class)

172. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

173. Defendant acquired and maintained the PII of Plaintiff and the Class including their Social Security numbers and other sensitive information to provide employment and/or medical services.

174. Plaintiff and Class Members reasonably expected that their PII that they entrusted to Integris, as part of their employment and/or medical services, would remain confidential and would not be shared or disclosed to criminal third parties.

175. Plaintiff 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 Plaintiff 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 that is not directly related to or beneficial to employment and elective benefits stemming therefrom.

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

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

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

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

180. Plaintiff 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 Plaintiff and the Class)

181. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

182. Plaintiff alleges this claim in the alternative to his breach of implied contract claim.

183. Plaintiff and the Class provided their PII to Integris to receive employment and/or medical services.

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

185. Through the collection and use of Plaintiff's and the Class's PII, Defendant was able to employ Plaintiff and Class Members and/or provide medical services. Through employment of Plaintiff and Class Members and/or providing medical services, Defendant was able to run its business and receive substantial revenue it otherwise would not have been able to receive.

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

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

188. 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 Plaintiff's 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 Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff 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.

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

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

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

192. Plaintiff and Class Members have no adequate remedy at law.

193. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity 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 Breaches, 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 remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect 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 Plaintiff and Class Members.

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

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

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

196. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

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

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

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

200. Upon reason and belief, Defendant still possesses the PII of Plaintiff and the Class members.

201. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members.

202. 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 Breaches to occur and go undetected and, thereby, prevent further attacks.

203. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff 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.

204. Actual harm has arisen in the wake of the Data Breaches regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff 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.

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

206. Plaintiff 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 segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and security checks; and

g. 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, Plaintiff 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 Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

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. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

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

Dated: December 29, 2023

Respectfully submitted,

/s/ William B. Federman

William B. Federman, OBA # 2853
Kennedy M. Brian, OBA # 34617
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
E:wbf@federmanlaw.com
E: kpb@federmanlaw.com

Bryan Bleichner *
Philip Krzeski*
CHESTNUT CAMBRONNE
100 Washington Ave South.
Minneapolis, MN 55401
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com
Attorney for Aaaron Zinck and the Putative Class

*Pro Hac Vice forthcoming