IN THE CHANCERY COURT OF HAMILTON COUNTY, TENNESSEE
TENTH JUDICIAL DISTRICT

HEIDI DAVIS, JAVELIN ALEXANDER, and **MINDIE HUNT,** individually, and on behalf of himself and all others similarly situated,	) Case No. 25-0083
Plaintiff,	) **DEMAND FOR JURY TRIAL**
v.	) Part 1
REGIONAL OBSTETRICAL CONSULTANTS,	)
Defendant.	)

AMENDED CLASS ACTION COMPLAINT

Plaintiffs, Heidi Davis, Javelin Alexander, and Mindie Hunt (collectively, "Plaintiffs") bring this Amended Class Action Complaint against Defendant Regional Obstetrical Consultants, P.C. ("Defendant"), individually, and on behalf of all others similarly situated, allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard the sensitive, personal information of Plaintiffs and other similarly situated current and former patients' ("Class Members," defined *infra*), including their personally identifiable information ("PII") including names, dates of birth, addresses, phone numbers, and protected health information ("PHI") including medical record number, insurance ID number, diagnosis, medical history, and procedures (together with PHI, "Private Information").

2. Defendant is a medical practice offering "a wide range of services in the areas of

Maternal-Fetal Medicine, sonography, ultrasound, and prenatal diagnostics and screenings."[1]

3. Defendant received Plaintiffs' and Class Members' Private Information in its provision of medical services to Plaintiffs and Class Members.

4. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about May 6, 2024, Defendant's network had been accessed and acquired by an unauthorized third party ("Data Breach"). In the Data Breach, the Private Information of approximately 25,650 individuals was unauthorizedly disclosed and/or compromised, resulting in widespread injury and damages as set forth herein.[2]

6. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its patients' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

7. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate

---

[1] https://www.rocob.com/services/what-we-do (last visited Jan. 31, 2025).
[2] *See* U.S. Dep't of Health and Human Servs., Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

information security practices; and (iii) effectively secure its network containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and/or other tortious conduct, breach of contractual obligations, and violations of statutes.

8. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

9. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

10. Plaintiffs and Class Members have suffered injury as a result of Defendant's misconduct, including, *inter alia*: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information

was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

11. Plaintiff Heidi Davis is and was, at all times material hereto, a resident and citizen of the State of Georgia, with a principal residence in Calhoun, Georgia, where she intends to remain.

12. Plaintiff Javelin Alexander is and was, at all times material hereto, a resident and citizen of the State of Georgia, with a principal residence in Calhoun, Georgia, where she intends to remain.

13. Plaintiff Mindie Hunt is and was, at all times material hereto, a resident and citizen of the State of Georgia, with a principal residence in Tunnel, Georgia, where she intends to remain.

14. Defendant is a Tennessee corporation with its principal place of business located at 902 McCallie Ave, Chattanooga, Tennessee 37403.

JURISDICTION AND VENUE

15. The Court has general subject matter jurisdiction over this action pursuant to Tenn. Code Ann. § 16-11-102.

16. This Court has personal jurisdiction over Defendant because it resides and operates a substantial portion of its business in this State.

17. Venue is proper in this Court under Tenn. Code Ann. § 20-4-101(c) because Defendant's principal place of business in this County.

FACTUAL ALLEGATIONS

A. Background

18. Defendant provides a wide range of medical services, including prenatal

diagnostics, ultrasounds, genetic counseling, and prenatal screening.[3]

19. Plaintiffs provided their Private Information to Defendant in connection with services they received from Defendant.

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

21. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiffs and Class Members, that their Private Information would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

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

23. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

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

25. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

---

[3] https://www.rocob.com/services/what-we-do (last visited Aug. 20, 2025).

26. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

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

B. The Data Breach

28. On January 22, 2025, Defendant announced that an unauthorized actor gained access to its network and acquired Private Information.

29. The Notice of Data Security Incident posted on Defendant's website states:

> Regional Obstetrical Consultants PC ("ROC" or "we") is providing notice of an event that may affect the privacy of certain individuals' information. ROC takes this Event very seriously and is providing information about the Event, the response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.
>
> **What Happened?** On May 6, 2024, ROC detected suspicious activity in its network environment. Upon discovery of this incident, ROC promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, ROC learned that an unauthorized actor accessed certain files and data stored within its network environment. Upon learning this, ROC began a time-consuming and detailed reconstruction and review of the potentially impacted data at the time of this incident to understand whose information may be affected. On December 23, 2024, ROC identified persons whose sensitive data may have been included within the impacted data.
>
> **What Information Was Involved?** ROC is notifying impacted individuals and providing information and resources to help protect individuals' personal information. The following types of information may have been impacted: name, address, phone number, date of birth, Social Security number, driver's license information, financial account information, patient account number/medical record number, health insurance plan or policy information, prescription drug information, lab test results or images, and/or medical diagnosis and treatment information. Not

all individuals had all of the above data elements impacted, the data impacted varies by individual.

What ROC Is Doing. ROC takes this event and the security of personal information in its care very seriously. Upon learning of this event ROC moved quickly to investigate and respond to the event and notify potentially affected individuals. As part of its ongoing commitment to the security of information, ROC is reviewing and enhancing its existing policies and procedures related to data privacy to reduce the likelihood of a similar future event. ROC is notifying impacted individuals for whom ROC has a valid mailing address via U.S. mail and offering them credit monitoring and identity protection services. ROC is also notifying applicable regulators.[4]

30. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

31. The attacker accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

32. Plaintiffs further believe their Private Information, and that of Class Members, was subsequently posted to and sold on the Dark Web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

33. Although Defendant detected the Data Breach in May 2024, it waited until July 2, 2024 to report the breach to the U.S. Department of Health and Human Services, Office for Civil Rights, then reporting that 25,650 individuals were affected in the Data Breach.[5]

---

[4] *See* Regional Obstetrical Consultants, *Notice of Data Privacy Event*, Jan. 22, 2025, https://www.rocob.com/storage/app/media/00-ROC-Website-Notice.pdf (last visited May 29, 2025).

[5] *See* U.S. Dep't of Health and Human Servs., Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

34. To add insult to injury, it was not until late January 2025 that Defendant notified the public of the Data Breach via an online posting[6] and began notifying Plaintiffs and the Class that their Private Information had been compromised in the Data Breach via written, mailed notice.

C. Defendant Acquires, Collects, and Stores the Private Information of Plaintiffs and Class Members

35. Defendant derives a substantial economic benefit from providing medical services to its patients, and as a part of providing that service, Defendant retains and stores Plaintiffs' and Class Members' Private Information.

36. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the Private Information from disclosure.

37. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

38. Defendant's patients, including Plaintiffs and Class Members, relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

39. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

40. Upon information and belief, Defendant made promises to Plaintiffs and Class Members to maintain and protect Plaintiffs' and Class Members' Private Information,

---

[6] *See* Regional Obstetrical Consultants, *Notice of Data Privacy Event*, Jan. 22, 2025, https://www.rocob.com/storage/app/media/00-ROC-Website-Notice.pdf (last visited May 29, 2025).

demonstrating an understanding of the importance of securing Private Information.

41. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of Private Information are Particularly Susceptible to Cyber Attacks.

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

43. Data thieves regularly target institutions like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

44. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[7]

45. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information it collected and maintained would be targeted by cybercriminals.

46. As a custodian of Private Information, Defendant knew, or should have known, the

---

[7] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022), https://notified.idtheftcenter.org/s/, at 6.

importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

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

48. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially tens of thousands of individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

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

E. Value of Personally Identifiable Information

51. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other

[8] 17 C.F.R. § 248.201 (2013).

things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

52. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[10]

53. For example, Private Information can be sold at a price ranging from $40 to $200.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

54. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[13]

55. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a "cyber black market" exists

---

[9] *Id.*
[10] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[12] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.
[13] *Medical I.D. Theft*, https://efraudprevention.net/home/education/?a= 187.

where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

56. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[14] Indeed, during 2019 alone, over 41 million health care records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[15] In short, these sorts of data breaches are increasingly common, especially among health care systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[16]

57. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[17]

58. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[18]

59. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-

---

[14] Adil Hussain She, et al., *Healthcare Data Breaches: Insights and Implications* (May 13, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/.
[15] Steve Adler, *December 2019 Healthcare Data Breach Report* (Jan 21, 2020), https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.
[16] Rody Quinlan, *Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era Breaches*, TENABLE BLOG (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.
[17] [17] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.
[18] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

pocket costs for health care they did not receive to restore coverage.[19] Almost half of medical identity theft victims lose their health care coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[20]

60. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—PHI and names—is impossible to "close" and difficult, if not impossible, to change.

61. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[21]

62. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

63. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for

---

[19] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[20] *Id.; see also* Brian O'Connell, *Healthcare Data Breach: What to Know About them and What to Do After One*, https://www.healthcarefacilitiestoday.com/posts/Healthcare-data-breach-What-to-know-about-them-and-what-to-do-after-one--18729.
[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

> 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.[22]

F. Defendant Failed to Comply with FTC Guidelines.

64. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

65. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

66. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the

---

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

network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

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

68. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

69. Defendant was at all times fully aware of its obligation to protect the Private Information of consumers under the FTCA, yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

G. Defendant Failed to Comply with HIPAA Guidelines.

70. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health

Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

71. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

72. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

73. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

74. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

75. "Electronic protected health information" is "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

76. HIPAA's Security Rule requires defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

77. HIPAA also requires Defendant to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

78. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. §17902.

79. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

80. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

81. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the

covered entity or its business associate. See 45 C.F.R. § 164.530(f).

82. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.

83. Defendant was at all times fully aware of its HIPAA obligations to protect the Private Information of consumers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

H. Defendant Failed to Comply with Industry Standards.

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

85. Some industry best practices that should be implemented by institutions dealing

with sensitive Private Information, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

86. Other best cybersecurity practices that are standard at large institutions that store Private Information include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

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

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

I. Defendant Breached Its Duty to Safeguard Plaintiffs' and Class Members' Private Information.

89. Defendant owed duties to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized

persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

90. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect consumers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to adhere to industry standards for cybersecurity as discussed above; and

e. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

91. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems and acquire unsecured and unencrypted Private Information.

92. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

J. Common Injuries & Damages

93. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including, but not limited to: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; € invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

K. The Data Breach Increases Victims' Risk of Identity Theft.

94. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

95. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

96. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other

criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

97. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

98. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

99. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Full" packages.[23]

---

[23] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

100. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

101. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

L. Loss of Time to Mitigate Risk of Identity Theft and Fraud

102. Because of the recognized risk of identity theft after a data breach, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

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

104. These efforts are consistent with the U.S. Government Accountability Office's 2007 report that data breaches ("GAO Report") result in victims of identity theft that will face "substantial costs and time to repair the damage to their good name and credit record."[24]

105. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[25]

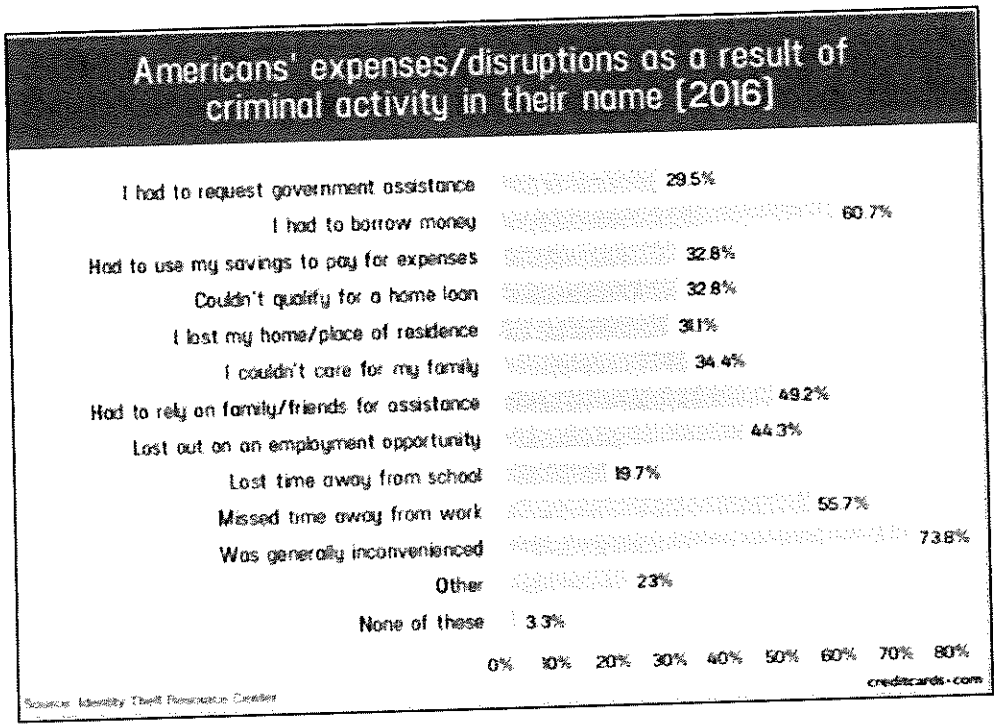
106. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[26]

---

[24] *See* U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

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

[26] Jason Steele, *Credit Card and ID Theft Statistics* (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



M. Diminution of Value of Private Information

107. PII and PHI are valuable property rights.[27] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that Private Information has considerable market value.

108. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[28]

109. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and

---

[27] *See, e.g.*, Randall T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[28] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

provides it to marketers or app developers.[29,30]

110. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[31]

111. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

112. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

113. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if their data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

114. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network, amounting to hundreds of thousands of individuals'

---

[29] https://datacoup.com/.
[30] https://digi.me/what-is-digime/.
[31] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

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

116. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes.

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

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

O. Plaintiffs' Experiences

Plaintiff Heidi Davis

119. Plaintiff Heidi Davis ("Plaintiff Davis") is a former patient of Defendant and provided her Private Information to Defendant in exchange for, and as a material condition of

receiving, medical services from Defendant.

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

121. Plaintiff Davis received a Notice Letter dated January 22, 2025 from Defendant informing her that her Private Information was included in the Data Breach.

122. Plaintiff Davis's Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

123. Plaintiff Davis takes reasonable measures to protect her Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

124. Plaintiff Davis stores any documents containing her Private Information in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

125. As a result of the Data Breach, Plaintiff Davis has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

126. Plaintiff Davis also suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that she entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

127. Since the Data Breach, Plaintiff Davis has experienced an increase in spam calls

and texts, resulting from the misuse of her Private Information unauthorizedly disclosed in the Data Breach.

128. Plaintiff Davis suffered lost time, interference, and inconvenience as a result of the Data Breach.

129. Plaintiff Davis has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her name, date of birth, and PHI, being placed in the hands of criminals.

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

131. As a result of the Data Breach, Plaintiff Davis anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Davis is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Javelin Alexander

132. Plaintiff Javelin Alexander ("Plaintiff Alexander") is a former patient of Defendant and provided her Private Information to Defendant in exchange for, and as a material condition of receiving, medical services from Defendant.

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

134. Plaintiff Alexander received a Notice Letter dated January 22, 2025 from Defendant informing her that her Private Information was included in the Data Breach, including her name,

date of birth, address, insurance ID number, diagnosis, and procedures.

135. Plaintiff Alexander's Private Information was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

136. Plaintiff Alexander takes reasonable measures to protect her Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

137. Plaintiff Alexander stores any documents containing her Private Information in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

138. As a result of the Data Breach, Plaintiff Alexander has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

139. Plaintiff Alexander also suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that she entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

140. Since the Data Breach, Plaintiff Alexander has experienced an increase in spam calls and texts, resulting from the misuse of her Private Information unauthorizedly disclosed in the Data Breach.

141. Plaintiff Alexander suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

142. Plaintiff Alexander has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, especially her name, date of birth, and PHI, being placed in the hands of criminals.

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

144. As a result of the Data Breach, Plaintiff Alexander anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Alexander is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Mindie Hunt

145. Plaintiff Mindie Hunt ("Plaintiff Hunt") is a former patient of Defendant and provided her Private Information to Defendant in exchange for, and as a material condition of receiving, medical services from Defendant.

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

147. Plaintiff Hunt received a Notice Letter dated January 22, 2025 from Defendant informing her that her Private Information was included in the Data Breach, including her name, date of birth, address, phone number, and protected health information ("PHI"), including medical record number, insurance ID number, diagnosis, medical history, and procedures.[32]

148. Plaintiff Hunt's Private Information was compromised in the Data Breach and

[32] *See* Exhibit A.

stolen by cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

149. Plaintiff Hunt takes reasonable measures to protect her Private Information. She has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

150. Plaintiff Hunt stores any documents containing her Private Information in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

151. As a result of the Data Breach, Plaintiff Hunt has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and work duties.

152. Plaintiff Hunt also suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that she entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

153. Since the Data Breach, Plaintiff Hunt has experienced an increase in spam calls and texts, resulting from the misuse of her Private Information unauthorizedly disclosed in the Data Breach.

154. Plaintiff Hunt suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

155. Plaintiff Hunt has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private

Information, especially her name, date of birth, and PHI, being placed in the hands of criminals.

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

157. As a result of the Data Breach, Plaintiff Hunt anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Hunt is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

158. Pursuant to the Tennessee Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and on behalf of all members of the proposed class defined as:

> **All individuals residing in the United States whose Private Information was disclosed or compromised in the Data Breach, including those individuals to whom Defendant sent notice of the Data Breach ("Class").**

159. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

160. Plaintiffs reserve the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

161. The proposed Class satisfies the numerosity, commonality, typicality, and adequacy requirements under Tenn. R. Civ. P. 23.01(1)-(4).

162. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believe the proposed Class includes approximately 25,650 individuals,[33] according to Defendant, who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendant's records.

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

a. Whether Defendant engaged in the conduct alleged herein;

b. When Defendant learned of the Data Breach;

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

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

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

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

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

[33] *See* U.S. Dep't of Health and Human Servs., Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

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

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

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

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

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

m. Whether Defendant's conduct was negligent;

n. Whether Defendant was negligent *per se*;

o. Whether Defendant breached contracts it had with its patients, including Plaintiffs and Class Members;

p. Whether Defendant was unjustly enriched;

q. Whether Defendant invaded Plaintiffs' and the Class Members' privacy;

r. Whether Defendant owed fiduciary duties to Plaintiffs and the Class;

s. Whether Defendant breached its fiduciary duties;

t. Whether Plaintiffs and Class Members are entitled to damages;

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

v. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the

establishment of a constructive trust.

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

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

166. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members. For example, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

167. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

168. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

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

169. Plaintiffs incorporate paragraphs 1 through 168, as if fully set forth herein.

170. Defendant's patients, including Plaintiffs and Class Members, provided their non-public Private Information to Defendant as a condition of obtaining services.

171. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was not adequately safeguarded and was wrongfully disclosed.

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

173. Defendant had duties to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

174. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the health care and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

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

177. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

178. Defendant breached its duties, pursuant to the common law and industry standards, the FTCA, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to

safeguard Plaintiffs' and Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

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

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

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

f. Failing to timely and adequately notify Plaintiffs and Class Members about the Data Breach's occurrence and scope, so they could take appropriate steps to mitigate the potential for identity theft and other damages.

179. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

180. Further, Defendant's violation of federal statutes and other applicable laws also constitutes negligence *per se*. Specifically, as described herein, Defendant has violated the FTCA and HIPAA.

181. Plaintiffs and Class Members were within the class of persons the FTCA and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

182. Defendant has admitted that the Private Information of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

184. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

185. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will imminently suffer injury and damages, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

186. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

187. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

188. Plaintiffs and Class Members are therefore entitled to damages, including compensatory and actual damages, restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses; and punitive damages, as permitted by law.

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

189. Plaintiffs incorporate paragraphs 1 through 168, as if fully set forth herein.

190. Plaintiffs and Class Members were required to deliver their Private Information to Defendant as part of the process of obtaining health care services provided by Defendant. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for health care services.

191. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

192. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

193. Plaintiffs and Class Members entrusted their Private Information to Defendant, along with monies paid for medical services. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such

information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

194. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

195. Implicit in the agreement between Plaintiffs and Class Members and Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

196. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

197. On information and belief, at all relevant times, Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

198. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

199. Plaintiffs and Class Members paid money to Defendant with the reasonable belief

and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

200. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

201. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

202. Tennessee law provides that every contract includes good faith and fair dealing between the parties involved.

203. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

204. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their Private Information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that Private Information was compromised as a result of the Data Breach

205. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

206. As a direct and proximate result of Defendant's breach of the implied contracts,

Plaintiffs and Class Members sustained injury and damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

207. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

208. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

209. Plaintiffs incorporate paragraphs 1 through 168, as if fully set forth herein.

210. This count is brought in the alternative to Plaintiffs' breach of implied contract claim (Count II).

211. Upon information and belief, Defendant funds its data security measures entirely

from its general revenue, including from payments made by and/or on behalf of its patients, including Plaintiffs and Class Members, in exchange for medical services, for which Defendant collected and maintained Plaintiffs' and Class Members' Private Information.

212. As such, a portion of the value and monies derived from Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

213. Plaintiffs and Class Members conferred a monetary benefit on Defendant by providing it with their valuable Private Information.

214. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' and Class Members' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

215. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit 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 profit over the requisite security.

216. Under the principles of equity and good conscience, Defendant should not be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

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

218. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class

Members have suffered and will suffer injury and damages, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

219. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiffs and Class Members may seek restitution or compensation.

COUNT IV
INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of Plaintiffs and the Class)

220. Plaintiffs incorporate paragraphs 1 through 168, as if fully set forth herein.

221. Plaintiffs and Class members took reasonable and appropriate steps to keep their Private Information confidential from the public.

222. Plaintiffs' and Class members' efforts to safeguard their own Private Information were successful, as their Private Information was not known to the general public prior to the Data Breach.

223. Plaintiffs and Class members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to

unauthorized third parties.

224. Defendant owed a duty to its patients, including Plaintiffs and Class members, to keep their Private Information confidential.

225. The unauthorized release of Private Information, especially dates of birth and medical information, is highly offensive to a reasonable person.

226. Plaintiffs' and Class members' Private Information is not of legitimate concern to the public.

227. Defendant knew or should have known that Plaintiffs' and Class members' Private Information was private, as it is subject to HIPAA and other laws described herein.

228. Defendant publicized Plaintiffs' and Class members' Private Information, by communicating it to cyber criminals who had no legitimate interest in this Private Information and who had the express purpose of monetizing that information by misusing it for fraudulent purposes or injecting it into the illicit stream of commerce flowing through the dark web.

229. Indeed, not only is Plaintiffs' and Class Members' Private Information traveling the dark web, but it is being used to commit fraud, as reflected by the spam communications received by Plaintiffs; and, on information and belief, it is being disseminated amongst, *inter alia*, merchants, creditors, health care providers and governmental agencies.

230. It is therefore likely that the Plaintiffs' and the Class Members' Private Information is rapidly becoming public knowledge–among the community writ large–due to the nature of the malware attack that procured it, and the identity theft that it is designed for.

231. Moreover, the publication was intentional under the definition of intent in Section 8A of the Restatement (Second) of Torts because, given the ubiquity of data breaches, Defendant was substantially certain that its decision to forego reasonable cybersecurity measures would lead

to a data breach.

232. Further, the publication requirement is met because the disclosure was to cybercriminals and identity thieves who are in a special relationship with Plaintiffs and the Class in that they are the exact group of people from whom reasonable cybersecurity measures are intended to protect Plaintiffs and the Class.

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

234. As a direct and proximate result of Defendant's invasion of privacy, Plaintiffs and Class Members have suffered and will suffer injury and damages, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Heidi Davis, Javelin Alexander, and Mindie Hunt, individually, and on behalf of all others similarly situated, request judgment against Defendant and that the

Court grant the following:

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

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

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

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

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

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

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive

Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

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

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

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

information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

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

xvi. for a period of 10 years, appointing a qualified and independent third-party

assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

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

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

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: September 8, 2025

Respectfully submitted,

J. Gerard Stranch, IV (BPR 23045)
Grayson Wells (BPR 039658)
Miles Schiller (BPR 041531)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Ave., Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com
mschiller@stranchlaw.com

Jeff Ostrow*
Ken Grunfeld*
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com
grunfeld@kolawyers.com

Alexandra M. Honeycutt
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Tel: (865) 247-0080
ahoneycutt@milberg.com

Eduard Korsinsky*
Melissa Meyer*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 27th Floor
New York, NY 10004
Tel: (212) 363-7500
ek@zlk.com
mmeyer@zlk.com

**Pro hac vice forthcoming*

Counsel for Plaintiffs and the Putative Class

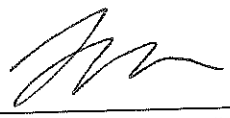
CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 9th day of September, 2025, the foregoing Amended Class Action Complaint was served by U.S. Mail, and/or electronic mail, to the following:

David Ross
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP
1500 K Street NW, Suite 330
Washington, D.C. 20005
Tel: 202-626-7660
David.ross@wilsonelser.com

Matthew Foree
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP
3348 Peachtree Road NE, Suite 1400
Atlanta, GA 30326
Tel: 470-666-5704
Matthew.foree@wilsonelser.com

Counsel for Defendant Regional Obstetrical Consultants, P.C.



J. Gerard Stranch, IV (BPR 23045)

Exhibit A

Regional Obstetrical Consultants PC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998
Via First-Class Mail

PL9IY200200606
MINDIE HUNT
[redacted]
TUNNEL, GA 30755-9779

REGIONAL OBSTETRICAL CONSULTANTS

January 22, 2025

PL9IY200200606060601028140

Notice of Data Event

Dear Mindie Hunt:

Regional Obstetrical Consultants PC ("ROC" or "we") writes to inform you of a recent event that may impact some of your information. ROC takes this event seriously and the privacy, security, and confidentiality of information in our care is among our highest priorities. While ROC is not aware of any actual or attempted misuse of your information to perpetrate financial fraud, out of an abundance of caution, we are providing you with an overview of the event, our response, and resources to help further protect your information, should you feel it necessary to do so.

What Happened?

On May 6, 2024, ROC detected suspicious activity in its network environment. Upon discovery of this incident, ROC promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, ROC learned that an unauthorized actor accessed certain files and data stored within its network environment.

Upon learning this, ROC began a time-consuming and detailed reconstruction and review of the potentially impacted data at the time of this incident to understand whose information may be affected. On December 23, 2024, ROC identified persons whose sensitive data may have been included within the impacted data.

What Information Was Involved?

ROC determined that the information related to you that may have been copied without authorization as a result of the incident: Name, Date of Birth, Medical Record Number, Insurance ID Number, Address, Phone Number, Diagnosis, Medical History, Procedures.

What We Are Doing?

The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of the event, we moved promptly to investigate and respond to the event and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. As an added precaution, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. While the ROC is covering the cost of these services, you will need to complete the activation process yourself.