AlaFile E-Notice

01-CV-2024-903135.00

To: JONATHAN S. MANN
jonm@pittmandutton.com

NOTICE OF ELECTRONIC FILING

IN THE CIRCUIT COURT OF JEFFERSON COUNTY, ALABAMA

TAMMY BROWN V. ALABAMA CARDIOLOGY GROUP, P.C. D/B/A ALABAMA CARDIOVASC
01-CV-2024-903135.00

The following complaint was FILED on 12/30/2024 6:07:28 PM

Notice Date: 12/30/2024 6:07:28 PM

JACQUELINE ANDERSON SMITH
CIRCUIT COURT CLERK
JEFFERSON COUNTY, ALABAMA
716 RICHARD ARRINGTON, JR BLVD
BIRMINGHAM, AL, 35203

205-325-5355
jackie.smith@alacourt.gov

ELECTRONICALLY FILED
12/30/2024 6:07 PM
01-CV-2024-903135.00
CIRCUIT COURT OF
JEFFERSON COUNTY, ALABAMA
JACQUELINE ANDERSON SMITH, CLERK

IN THE CIRCUIT COURT OF JEFFERSON COUNTY, ALABAMA
BIRMINGHAM DIVISION

TAMMY BROWN, VANESSA BROOKS, EMILY SMITH SANDERS, and ASHLEY OAKES, individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	**Case No.: 01-CV-2024-903135**
v.	)	
ALABAMA CARDIOLOGY GROUP, P.C. d/b/a **ALABAMA CARDIOVASCULAR GROUP,**	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Tammy Brown, Vanessa Brooks, Emily Smith Sanders and Ashley Oakes (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, file this Consolidated Class Action Complaint, pursuant to the Court's November 14, 2024 Order, against Defendant Alabama Cardiology Group, P.C. d/b/a Alabama Cardiovascular Group ("ACG" or "Defendant") and allege the following based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against ACG for its failure to properly secure and safeguard Plaintiffs' and Class Members' (defined below) highly sensitive personally identifiable information ("PII"), protected health information ("PHI"), as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), and other medical and financial information,

(collectively, "PHI/PII" or "Private Information") from criminal hackers.

2. ACG is a privately owned cardiovascular and cardiology medical practice group comprised of over twenty-five (25) physicians and nurse practitioners who treat patients in central Alabama at their main office at Grandview Medical Center in Birmingham and at their satellite offices in Columbiana, Gadsden, Homewood, Pell City, Sylacauga, and Trussville.[1]

3. On or about August 2, 2024, ACG filed an official notice of a hacking incident with the Massachusetts Attorney General's Office[2] and sent data breach notification letters[3] (the "Notice") to Plaintiffs and over 280,000 individuals[4], who were current and former patients (including ***minor dependents***), guarantors, employees, and physicians at ACG, detailing that unauthorized third parties accessed to its network that contained their highly sensitive PII/PHI.

4. Based on the Notice sent to Plaintiffs and Class Members, unusual activity was detected on some of its computer systems. In response, Defendant initiated an investigation. ACG's investigation revealed that an unauthorized party had access to certain files that contained sensitive patient information (the "Data Breach").

5. Due to ACG's highly inadequate cybersecurity policies, practices and procedures, hackers had unfettered access to ACG's network and systems for over twenty-five (25) days, as the Notice admits that "ACG's investigation determined that between June 6, 2024 and July 2, 2024, unauthorized parties gained access to the ACG network and obtained personal information."

---

[1] *See Contact Us*, ALABAMA CARDIOVASCULAR GROUP, http://www.alcardio.com/contact.aspx and *Our Physicians*, ALABAMA CARDIOVASCULAR GROUP, https://alcardio.com/physicians.html . (last visited Dec. 27, 2024).
[2] *Data Breach Notice*, MASS.GOV (Aug. 2, 2024) https://www.mass.gov/doc/2024-1412-alabama-cardiovascular-group/download.
[3] *Data Breach Notice*, MASS.GOV (Aug. 2, 2024) https://www.mass.gov/doc/2024-1412-alabama-cardiovascular-group/download.
[4] *Cases Currently Under Investigation*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 18, 2024).

A copy of the data breach notification letter that ACG sent to impacted individuals is attached hereto as **Exhibit A**.

6. Plaintiffs and Class Members were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, full name, Social Security numbers, date of birth, address, email, driver's license or passport number, financial information (credit or debit card information and/or bank account information), medical information (dates of service, diagnosis, medications, images, lab results, treatment information), health insurance information that ACG collected and maintained.

8. This Data Breach was a direct result of ACG's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiffs' and Class Members' PII/PHI.

9. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. ACG disregarded the rights of Plaintiffs and Class Members by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its

data networks, systems and/or servers were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Patients' PII/PHI; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach; and failing to provide comprehensive and effective credit protection services after notification of the Data Breach.

11. As a result of ACG's failure to implement and follow basic security procedures, Plaintiffs' and Class Members' PII/PHI is now in the hands of thieves who, upon information and belief, have committed criminal acts against them by misusing their data and/or have published and/or sold their data on the internet (i.e., the "dark web") for others to view, access, and/or misuse. Plaintiffs and Class Members have had to spend, and will continue to spend, significant amounts of time and money to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and financial fraud.

12. Plaintiffs, on behalf of all other citizens of Alabama similarly situated, allege claims for negligence, wantonness, negligence *per se*, breach of express and/or implied contracts, breach of fiduciary duty, and unjust enrichment and seek to compel ACG to fully and accurately disclose the nature of the Data Breach and the information that has been compromised, in addition to adopting sufficient security practices and protocols to safeguard the Patients' PII/PHI that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future, because the risk of future harm from another ACG data breach is both imminent and substantial.

13. ACG disclosed to its Patients that unauthorized third parties had access to its networks and servers for over three (3) weeks, which was more than sufficient time to obtain and

steal Plaintiffs' and Class Members' PII/PHI, leading to an imminent and substantial risk of identity theft and other misuse of the Plaintiffs' information.

14. ACG flagrantly disregarded Plaintiffs' and the other Class Members' privacy rights by intentionally, willfully, recklessly, negligently and/or wantonly failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized disclosure.

15. Plaintiffs' and Class Members' PII/PHI was improperly handled and stored and was otherwise not kept in accordance with federally prescribed, industry standard security practices and procedures. As a result, Plaintiffs' and Class Members' PII/PHI was compromised, accessed, and stolen.

16. ACG's intentional, willful, reckless, negligent and/or wanton disregard of Plaintiffs' and Class Members' rights directly and/or proximately caused a substantial unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI. The improper use of PII/PHI by unauthorized third parties resulted in an adverse impact on the credit rating and finances of Plaintiffs and the Class Members.

17. The type of wrongful PII/PHI disclosure made by ACG is the most harmful because it generally takes a significant amount of time for a data breach victim to become aware of misuse of that PII/PHI. Additionally, it takes a significant amount of time to protect oneself against attempted and actual identity theft and financial fraud.

18. On behalf of themselves and Class Members, Plaintiffs bring this lawsuit because they have suffered, and will continue to suffer, actual injuries and damages as a direct and/or proximate result of ACG's wrongful actions and/or inactions and the resulting Data Breach including, but not limited to, unauthorized disclosure, publication, and dissemination of their

PII/PHI on the internet, misuse of their PII/PHI, identity theft, financial fraud, loss of money and time in combatting the attempted and actual identity theft and fraud, and emotional distress.

19. Additionally, Plaintiffs seek injunctive relief as a direct and/or proximate result of ACG's wrongful actions and/or inactions to prevent ACG's next data breach, which is both likely and imminent.

20. ACG's wrongful actions and/or inactions and the resulting Data Breach have placed Plaintiffs and Class Members at an imminent, immediate, substantial, and continuing increased risk of identity theft and identity fraud.[5] Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released a 2012 Identity Fraud Report (the "Javelin Report") quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII/PHI is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported and a high probability that criminals who now possess Plaintiffs' and Class Members' PII/PHI—if they have not already misused the data—will do so later or re-sell it. Even if they are without such loss now, Plaintiffs and Class Members are entitled to relief and recovery because Plaintiffs and Class Members are under an imminent risk that their information will soon be misused similar to the misuse other Plaintiffs have already experienced.

21. Plaintiffs, on behalf of themselves and the Class Members, seek actual damages, economic damages, nominal damages, exemplary damages, injunctive relief, and costs of suit.

[5] According to the United States Government Accounting Office, the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as when PII/PHI is used to commit fraud or other crimes (credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services)).

22. There has been no assurance offered by ACG that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network and/or system in the future.

23. Plaintiffs bring this class action lawsuit to address ACG's inadequate safeguarding of Class Members' Private Information that it collected, stored, and maintained.

24. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to ACG, and thus ACG was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

25. Plaintiffs' and Class Members' identities are now at risk because of ACG's negligent and/or wanton conduct as the Private Information that ACG collected and maintained is now in the hands of data thieves and other unauthorized third parties.

26. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

27. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, wantonness, negligence *per se*, breach of implied contract, unjust enrichment, and breach of fiduciary duty.

II. PARTIES

28. Plaintiff Tammy Brown is, and at all times mentioned herein was, a resident and citizen of Walker County, Alabama.

29. Plaintiff Vanessa Brooks is, and at all times mentioned herein was, a resident and citizen of Shelby County, Alabama.

30. Plaintiff Emily Smith Sanders is, and at all times mentioned herein was, a resident and citizen of Blount County, Alabama.

31. Plaintiff Ashley Oakes is, and at all times mentioned herein was, an individual citizen of Etowah County, Alabama.

32. Defendant Alabama Cardiology Group, P.C. d/b/a Alabama Cardiovascular Group is a healthcare services company incorporated in Alabama with its principal place of business located at Grandview Medical Center, 3680 Grandview Parkway, Suite 200, Birmingham, Alabama. ACG conducts business in Jefferson County and throughout Alabama.

33. Whenever reference in this Complaint is made to any act or transaction of ACG, such allocations shall be deemed to mean that the principals, officers, employees, agents, and/or representatives of ACG committed, knew of, performed, authorized, ratified and/or directed such transaction on behalf of ACG while actively engaged in the scope of their duties.

III. JURISDICTION AND VENUE

34. Jurisdiction is proper in Alabama because, at all relevant times, ACG conducted (and continues to conduct) business in Alabama, each Plaintiff received health services and contracted with ACG to safeguard their PII and PHI in Alabama, Plaintiffs' PII/PHI was stored on ACG's computer networks, systems and/or servers in Alabama, many of ACGs wrongful acts and omissions took place in Alabama, and ACG's principal place of business is in Alabama.

35. Venue is proper in Jefferson County pursuant to Ala. Code § 6-3-7 because a substantial part of the events or omissions giving rise to this action occurred in Jefferson County, ACG's principal place of business is in Jefferson County, and ACG routinely conducts business throughout Jefferson County.

IV. FACTUAL ALLEGATIONS

A. *ACG's Business and Collection of Plaintiffs' and Class Members' Private Information*

36. ACG is a healthcare services provider. Founded in 2003, ACG specializes in ischemic, vascular and hypertensive heart disease as well as renal and peripheral vascular disease, throughout Alabama. Upon information and belief, ACG employs more than 50 people and generates approximately $16.3 million in annual revenue.

37. As a condition of receiving healthcare services, ACG requires that its patients (including minors) and guarantors entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from ACG, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

38. In its official "Privacy Policy," ACG promises its patients the following:

a. "We are required by law to maintain the privacy of your protected health information and to provide you with notice of our legal duties and privacy practices with respect to your protected health information."[6]

b. "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED[.]"[7]

c. "We are required to abide by the terms of our Notice of Privacy Practices ('Notice') currently in effect."[8]

d. "ALL OTHER USES AND DISCLOSURES OF YOUR PHI REQUIRES YOUR WRITTEN AUTHORIZATION."[9]

[6] *Privacy Policy*, ALABAMA CARDIOVASCULAR GROUP (April 14, 2003) http://alcardio.com/privacy.html.
[7] *Id*.
[8] *Id*.
[9] *Id*.

e. "We have set up reasonable safeguards that protect against impermissible uses and disclosures and limits incidental uses or disclosures."[10]

f. "We also have policies and procedures that set limits to ensure that, as applicable, only the reasonable minimum necessary amount of your PHI is used, disclosed and requested for certain purposes."[11]

39. Thus, due to the highly sensitive and personal nature of the information ACG acquires and stores with respect to its patients, ACG, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

40. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, ACG assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

41. Plaintiffs and Class Members relied on ACG to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

[10] *Id*.
[11] *Id*.

B. ***The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members***

42. According to Defendant's Notice, it learned of unauthorized access to its computer systems on July 2, 2024, with such unauthorized access having taken place between June 6 and July 2, 2024.[12]

43. To make matters worse, ACG already admitted that "unauthorized parties gained access to the ACG network and ***obtained*** personal information."[13]

44. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including the following:

a. names;

b. addresses;

c. email addresses;

d. phone numbers;

e. demographic information;

f. dates of birth;

g. Social Security numbers;

h. health insurance information;

i. health insurance claims information;

j. usernames and passwords;

k. medical information;

l. dates of service;

m. medical diagnoses;

[12] *Data Breach Notice*, MASS.GOV (Aug. 2, 2024) https://www.mass.gov/doc/2024-1412-alabama-cardiovascular-group/download.
[13] *Id*. (emphasis added).

n. medications;

o. images;

p. lab results;

q. treatment information;

r. driver's license numbers;

s. passport numbers;

t. credit card numbers;

u. debit card information; and

v. bank account information.[14]

45. On or about August 2, 2024, roughly one month after ACG learned that the Class's Private Information was first accessed by cybercriminals, ACG finally began to notify current and former patients and employees that its investigation determined that their Private Information was affected.[15]

46. In total, the Data Breach exposed the Private Information of 280,534 individuals (*i.e.*, Plaintiffs and Class Members).[16] Class Members include the "current or past patient[s] of a physician at ACG" and the "current or past patient guarantor[s], employee[s], or physician[s] at ACG."[17]

47. ACG had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

---

[14] *Id*.
[15] *Id*.
[16] *Cases Currently Under Investigation*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 18, 2024).
[17] *Data Breach Notice*, MASS.GOV (Aug. 2, 2024) https://www.mass.gov/doc/2024-1412-alabama-cardiovascular-group/download.

48. Plaintiffs and Class Members provided their Private Information to ACG with the reasonable expectation and mutual understanding that ACG would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

49. ACG's data security obligations were particularly important given the substantial increase in cyberattacks against healthcare providers, including cardiology clinics, in recent years.

50. ACG knew or should have known that its electronic records would be targeted by cybercriminals.

C. *The Healthcare Sector is Particularly Susceptible to Data Breaches*

51. ACG was on notice that companies in the healthcare industry are susceptible targets for data breaches.

52. In August 2014, after a cyberattack on Community Health Systems, Inc., the Federal Bureau of Investigation ("FBI") warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[18]

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

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning

[18] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014) https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

> that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[19]

54. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[20] In 2022, the largest growth in compromises occurred in the healthcare sector.[21]

55. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[22]

56. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[23]

57. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any

---

[19] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N. (Oct. 4, 2019) https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[20] *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_2018-EOY-BREACH-REPORT-KEY-FINDINGS.pdf (last visited on Nov. 15, 2024).

[21] *2022 End-of-Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on Nov. 15, 2024).

[22] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

[23] *Id*.

given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[24]

58. As a healthcare provider, ACG knew, or should have known, the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on ACG's patients as a result of a breach. ACG failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. ***ACG Failed to Comply with HIPAA***

59. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that HHS create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

60. ACG's Data Breach resulted from a combination of insufficiencies that indicate ACG failed to comply with safeguards mandated by federal statutes, HIPAA regulations and industry standards. First, it can be inferred from ACG's Data Breach that ACG either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

61. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

[24] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXECUTIVE (April 4, 2019) https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

62. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

63. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

64. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

65. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

66. Based upon Defendant's Notice to Plaintiffs and Class Members, ACG reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

67. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

68. ACG reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

69. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach,

and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

70. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

71. ACG reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

72. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

73. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

74. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

75. In addition, ACG's Data Breach could have been prevented if ACG had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

76. ACG's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information ACG creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to 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 in violation of 45 CFR 164.312(a)(1);

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

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

77. Because ACG has failed to comply with federal and state statutes and HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure ACG's approach to information security is adequate and appropriate going forward. ACG still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. ***ACG Failed to Comply with FTC Guidelines***

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

79. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[25] . The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies 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.

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

81. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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 Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

82. Such FTC enforcement actions include those against businesses that fail to

[25] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (October 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

adequately protect customer data, like ACG here. *See, e.g.*, *In the Matter of LabMD, Inc.*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

83. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like ACG of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of ACG's duty in this regard.

84. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[26]

85. As evidenced by the Data Breach, ACG failed to properly implement basic data security practices. ACG'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.

86. ACG was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[26] FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable*, FEDERAL TRADE COMMISSION (Dec. 7, 2009) https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

F. ***ACG Failed to Comply with Industry Standards***

87. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

88. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[27]

89. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old

[27] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on Nov. 15, 2024).

devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

90. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[28]

91. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including 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

[28] *Shields Up: Guidance for Organizations*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Nov. 15, 2024).

(CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

G. *ACG Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information*

92. In addition to its obligations under federal and state laws, ACG owed a duty 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, or misused by unauthorized persons. ACG 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

93. ACG breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent, reckless and/or wanton because it failed to properly maintain and safeguard its computer networks, systems, and data. ACG'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 patients' Private Information;

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

d. Failing to sufficiently train its employees regarding the proper handling of its patients Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to federal and state laws, HIPAA, and industry standards for cybersecurity as discussed above; and

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

94. ACG negligently and/or wantonly failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

95. Had ACG remedied the deficiencies in its information storage and security systems, followed basic 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.

96. Accordingly, Plaintiffs' and Class Members' were injured and their lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with ACG.

H. *Plaintiffs and Class Members are at a Significantly Increased and Substantial Risk of Fraud and Identity Theft as a Result of the Data Breach.*

97. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[29] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them

[29] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* FEDERAL TRADE COMMISSION (October 2018) https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

98. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

99. Because a person's identity is akin to a puzzle, 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 to otherwise harass or track the victim. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

100. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

101. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access

accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

102. One such example of how malicious actors may compile Private Information is through the development of "Fullz" packages.

103. ""Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach 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. These dossiers are known as "Fullz" packages.

104. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can 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. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

105. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

freeze on their credit, and correcting their credit reports.[30] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

106. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

107. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[31] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic of anxiety attacks.[32]

[30] *What To Do Right Away,* FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/steps (last visited Nov. 15, 2024).
[31] *2023 Consumer Impact Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024) https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf.
[32] *Id*. at pp 21-25.

108. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[33]

109. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

110. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[34]

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

112. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[35]

[33] *Warning Signs of Identity Theft,* FED. TRADE COMMISSION, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on Nov. 15, 2024).
[34] *Data Breaches: In the Healthcare Sector,* CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Nov. 15, 2024).
[35] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014) https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Nov. 15, 2024).

113. The ramifications of ACG's failure to keep its patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

114. Here, not only was sensitive medical information compromised, but financial information and Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

115. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[36]

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

116. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

117. Identity theft occurs when a person's PII/PHI, such as the person's name, address, date of birth, Social Security number, billing and mailing addresses, phone number, email, credit card information, and health information is used without his or her permission to commit fraud or

[36] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVT. ACCOUNTABILITY OFFICE (June 2007) https://www.gao.gov/assets/gao-07-737.pdf.

other crimes.[37]

118. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[38] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII]."[39]

119. The FTC estimates that the identities of as many as nine million Americans are stolen each year. *Id.*

120. As a direct and/or proximate result of the Data Breach, Plaintiffs and Class Members have been, and will continue to be, required to spend money and to take the time and effort to combat actual or suspected identity theft and fraud and also mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing "freezes" and "alerts" with the credit reporting agencies, reviewing, closing or modifying financial accounts, scrutinizing their credit reports and bank and credit accounts, and purchasing products to monitor their credit reports and financial accounts for unauthorized activity. Because Plaintiffs' and Class Members' PII/PHI were stolen and/or compromised, they also now face a significantly heightened and imminent risk of harm and identity theft.

121. Citizens of Alabama, like some of the members of the proposed class here, have

---

[37] *See* https://consumer.ftc.gov/articles/what-know-about-identity-theft#what_is (last visited November 28, 2023).

[38] Protecting Consumer Privacy in an Era of Rapid Change FTC Report (March 2012) (https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf) (last visited November 28, 2023).

[39] *Id*., at 11–12.

suffered particularly severe losses from cybercrimes lately. A recent news article explained:

> According to the latest data on internet crimes compiled by the Federal Bureau of Investigation, Alabama saw the single-highest average of losses to cybercrime per victim in 2022. Research on the data published Friday by the online security company VPNpro found that ***victims of cybercrimes in Alabama lost, on average, $50,670 in 2022***. A total of 4,893 victims were reported in Alabama that year for a combined loss of nearly $248,000,000.[40]

122. According to the FTC, identity theft is serious. "[Identity thieves] might steal your name and address, credit card, or bank account numbers, Social Security number, or medical insurance account numbers. And they could use them to buy things with your credit cards, get new credit cards in your name, open a phone, electricity, or gas account in your name, steal your tax refund, use your health insurance to get medical care, [or] pretend to be you if they are arrested."[41]

123. Theft of medical information, such as that included in the Data Breach here, is equally serious: "Medical identity theft is when someone uses your personal information—like your name, Social Security number, health insurance account number or Medicare number—to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care. If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[42]

124. Identity thieves also use Social Security numbers to commit other types of fraud. The GAO found that identity thieves use PII/PHI to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, while in the meantime

[40] *See* https://aldailynews.com/alabamians-see-highest-losses-to-cybercrime-in-nation-new-research-finds/ (last visited November 28, 2023) (emphasis added).

[41] *See* https://consumer.ftc.gov/articles/what-know-about-identity-theft#what_is (last visited November 28, 2023).

[42] *See* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited November 28, 2023).

causing significant harm to the victim's credit rating and finances, which places Plaintiffs at an increased and imminent risk of further future harm. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change, and their misuse can continue for years into the future.

125. Identity thieves use Social Security numbers to commit other types of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes and/or filing fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves obtain jobs using stolen Social Security numbers, rent houses and apartments, and/or obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

126. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.[43] Thus, a person whose PII/PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

127. Obtaining a new Social Security number, however, is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not

[43] *See* https://consumer.ftc.gov/articles/do-you-need-new-social-security-number (last visited November 28, 2023).

guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

128. Phone numbers are de facto identity documents, given the increasing reliance on using phone numbers as verification (*i.e.*, two-factor authentication to access basic web pages.). A loss of a person's phone number can be as much of, if not more of, a risk than loss of a social security number—resulting in increased scam calls or loss of ability to access a web page.

129. As a direct and/or proximate result of ACG's wrongful actions and/or inactions and the Data Breach, the thieves and/or their customers now have Plaintiffs' and Class Members' PII/PHI. As such, Plaintiffs and Class Members have not only already lost actual value but have been deprived, and will continue to be deprived, of the value of their PII/PHI.[44]

130. Plaintiffs' and Class Members' PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[45] Identity thieves and other cyber criminals openly post stolen Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available.

131. The Data Breach was a direct and/or proximate result of ACG's failure to implement and maintain appropriate and reasonable security procedures and practices to safeguard

---

[44] *See, e.g.,* John T. Soma, J. Zachary Courson, John Cadkin, *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); ABC News Report, http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2#.UGRgtq7yBR4 (last visited November 28, 2023).

[45] Companies, in fact, also recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. *See* 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).

and protect Plaintiffs' and Class Members' PII/PHI from unauthorized access, use, and/or disclosure, as required by various federal and state regulations and industry practices.

132. ACG flagrantly disregarded and/or violated Plaintiffs' and Class Members' privacy rights, and harmed them in the process, by not obtaining Plaintiffs' and Class Members' prior written consent to disclose their PII/PHI to any other person—as required by HIPAA and other pertinent laws, regulations, industry standards and/or internal company policies.

133. ACG flagrantly disregarded and/or violated Plaintiffs' and Class Members' privacy rights, and have harmed them in the process, by failing to establish and/or implement appropriate administrative, technical, and other safeguards required by both industry standards and the Alabama Data Breach Notification Act of 2018, Ala. Code 1975 § 8-38-3, to ensure the security and confidentiality of Plaintiffs' and Class Members' PII/PHI to protect against anticipated threats to the security or integrity of such information. ACG's security deficiencies allowed unauthorized individuals to access, remove from its servers and networks, disclose, and/or compromise the PII/PHI over two-hundred eighty thousand of its current and former patients—including Plaintiffs and Class Members.

134. ACG's wrongful actions and/or inactions directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII/PHI without their knowledge, authorization, and consent. As a direct and proximate result of ACG's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and Class Members have incurred injuries and damages in the form of, *inter alia*: (i) an increased and imminent risk of future harm; (ii) the untimely and/or inadequate notification of the Data Breach; (iii) improper disclosure, dissemination and publication of their PII/PHI; (iv) criminal misuse of their PII/PHI; (v) identity theft; (vi) financial fraud; (vii) loss of privacy; (viii) out-of-pocket expenses incurred to mitigate

the identity theft and financial fraud and the continued increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) economic losses relating to the theft of their PII/PHI; (x) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (xi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (xii) stress, anxiety and emotional distress. Plaintiffs' and Class Members' damages were foreseeable by ACG

135. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. ***Plaintiffs' and Class Members' Damages***

Plaintiff Tammy Browns's Experience

136. Plaintiff Tammy Brown is a former patient of ACG—having received medical services over ***two decades ago*** in the 1990s.

137. Thus, ACG obtained and maintained Plaintiff Brown's PII/PHI since the 1990s.

138. ACG has maintained Plaintiff Brown's and Class Members' PII/PHI unprotected, unguarded, and/or unsecured.

139. Upon information and belief, Plaintiff Brown and Class Members' PII/PHI was stored unencrypted.

140. As a result, Plaintiff Brown was injured by ACG's Data Breach.

141. As a condition of receiving medical services, Plaintiff Brown provided ACG with her PII/PHI. ACG used that PII/PHI to facilitate its provision of medical services.

142. Plaintiff Brown provided her PII/PHI to ACG and trusted the company would use reasonable measures to protect, safeguard and secure it according to ACG's internal policies, as

well as state and federal law. ACG obtained and continues to maintain Plaintiff Brown's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

143. Plaintiff Brown reasonably understood that a portion of the funds paid to ACG would be used to pay for adequate cybersecurity and protection of PII/PHI.

144. Plaintiff Brown does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

145. Plaintiff Brown received a Notice of Data Breach on August 6, 2024.

146. Thus, on information and belief, Plaintiff Brown's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

147. Through its Data Breach, ACG compromised Plaintiff Brown's PII/PHI.

148. Plaintiff Brown has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, ACG directed Plaintiff to take those steps in its breach notice. Notably, Plaintiff has spent time contacting her bank and credit card company about the Data Breach.

149. Additionally, Plaintiff Brown received notification from the Internal Revenue Service after being notified of the Data Breach that another person used her Social Security Number to obtain employment.

150. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam phone calls.

151. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

152. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

153. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

154. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that ACG was required to adequately protect.

155. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because ACG's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

156. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

157. To date, Plaintiff Brown has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Brown values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

158. Plaintiff Brown suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (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) nominal damages; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

159. The Data Breach has caused Plaintiff Brown to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

160. As a result of the Data Breach, Plaintiff Brown is and will continue to be at increased risk of identity theft and fraud for years to come.

161. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in ACG's possession—is protected and safeguarded from additional breaches.

Plaintiff Vanessa Brooks' Experience

162. Plaintiff Brooks is a current patient of ACG. As a condition of receiving services from ACG, Plaintiff Brooks was required to provide Defendant with her Private Information. When providing her Private Information, Plaintiff Brooks reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

163. Plaintiff Brooks received ACG's Data Breach Notice. The Notice informed Plaintiff Brooks that her Private Information was improperly accessed and obtained by third parties.

164. After the Data Breach, in mid-August 2024, Plaintiff received notification of unauthorized charges on her bank card. Further, following the Data Breach, Plaintiff Brooks has noticed a significant increase in spam phone calls, emails, and text messages.

165. As a result of the Data Breach, Plaintiff Brooks has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Brooks has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

166. As a result of the Data Breach, Plaintiff Brooks has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her Private Information for purposes of identity theft and fraud. Plaintiff Brooks is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

168. As a result of the Data Breach, Plaintiff Brooks anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data

Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Emily Smith Sanders' Experience

169. Plaintiff Sanders was a patient of ACG in 2016. As a condition of receiving service from ACG, Plaintiff Sanders was required to provide Defendant with her Private Information. When providing her Private Information, Plaintiff Sanders reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

170. Plaintiff Sanders received ACG's Data Breach Notice. The Notice informed Plaintiff Sanders that her Private Information was improperly accessed and obtained by third parties.

171. Following the Data Breach, Plaintiff Sanders has noticed a significant increase in spam phone calls, emails, and text messages.

172. As a result of the Data Breach, Plaintiff Sanders has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Sanders has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

173. As a result of the Data Breach, Plaintiff Sanders has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling and using her Private Information for purposes of identity theft and fraud. Plaintiff Sanders is

concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

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

Plaintiff Ashley Oakes Experience

176. Plaintiff Oakes was a patient of ACG in 2022. As a condition of receiving service from ACG, Plaintiff Oakes was required to provide Defendant with her Private Information. When providing her Private Information, Plaintiff Oakes reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

177. On or about August 2, 2024, Plaintiff Oakes received a letter entitled "Important Security Notification" which told her that her Private Information had been affected during the Data Breach. This Notice informed her that the Private Information stolen included her "name, address, email, phone number, demographic information, date of birth, Social Security number, health insurance information and claims information, username and passwords, and medical information.".

178. The Notice letter offered Plaintiff Oakes only two years of credit monitoring services. Two years of credit monitoring is not sufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

179. Plaintiff Oakes suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

180. Plaintiff Oakes would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its patients' personal and health information from theft, and that those systems were subject to a data breach.

181. Plaintiff Oakes suffered an actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach. Additionally, after the Data Breach, Plaintiff Oakes received a notification from her financial institution that fraudsters made attempted withdrawals from her account.

182. Plaintiff Oakes suffered actual injury in the form of damages to and diminution in the value of her personal, health, and financial information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

183. Plaintiff Oakes suffered an imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

184. Plaintiff Oakes has a continuing interest in ensuring that her PII and PHI, which remain in the possession of Defendant, are protected and safeguarded from future breaches.

185. As a result of the Data Breach, Plaintiff Oakes made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

186. As a result of the Data Breach, Plaintiff Oakes has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

187. Plaintiff Oakes also suffered an actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

188. As a result of the Data Breach, Plaintiff Oakes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

189. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

190. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

191. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which the Data Breach resulted from Defendant's inadequate data security practices.

192. As a direct and proximate result of ACG's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

193. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

194. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

195. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

196. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

197. Plaintiffs and Class Members also lost the benefit of the bargain they made with ACG. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to ACG was intended to be used by ACG to fund adequate security of ACG's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive the benefit of the bargain.

198. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[46] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[47]

199. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and

[46] *See How Data Brokers Profit from the Data We Create*, THE QUANTUM RECORD, https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/ (last visited on Nov. 15, 2024).

[47] *Frequently Asked Questions,* NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Nov. 15, 2024).

the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

200. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

201. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of ACG, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

202. As a direct and proximate result of ACG's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

203. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Alabama Rules of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

204. Specifically, Plaintiffs propose the following Class, subject to amendment as appropriate:

> All Alabama citizens who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

205. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

206. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

207. The putative Class is comprised of persons who are citizens of many different counties of Alabama, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

208. The rights of each Class Member were violated in a virtually identical manner as a result of ACG's willful, reckless, negligent and/or wanton actions and/or inactions.

209. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a. Whether ACG willfully, recklessly, negligently and/or wantonly failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class Members' PII/PHI;

b. Whether ACG was negligent or wanton in the manner in which it stored Plaintiffs' and Class Members' PII/PHI;

c. Whether ACG owed a duty to Plaintiffs and Class Members to exercise reasonable care in protecting and securing their PII/PHI;

d. Whether ACG breached its duty to exercise reasonable care in protecting and securing Plaintiffs' and Class Members' PII/PHI;

e. Whether ACG was negligent in failing to secure Plaintiffs' and Class Members' PII/PHI;

f. Whether ACG failure to comply with federal laws, including HIPAA, constitutes negligence *per se*;

g. Whether ACG's failure to comply with Section 5 of the Federal Trade Commission Act (15 U.S.C. §45) constitutes negligence *per se*;

h. Whether ACG breached its contracts by failing to maintain the privacy and security of Plaintiffs' and Class Members' PII/PHI;

i. Whether by publicly disclosing Plaintiffs' and Class Members' PII/PHI without authorization, ACG invaded Plaintiffs' and Class Members' privacy;

j. Whether by publicly disclosing Plaintiffs' and Class Members' PII/PHI without authorization, ACG breached the duty of confidence it owed to Plaintiffs and Class Members;

k. Whether by publicly disclosing Plaintiffs' and Class Members' PII/PHI without authorization, ACG breached the fiduciary duties it owed to Plaintiffs and Class Members;

l. Whether ACG was unjustly enriched when it took money from Plaintiffs and Class Members and failed to provide reasonable data security measures to protect Plaintiffs' and Class Members' PII/PHI;

m. Whether Plaintiffs and Class Members sustained damages as a result of ACG's failure to secure and protect their PII/PHI; and

n. Whether injunctive relief is necessary to ensure ACG implements reasonable security measures to protect the PII/PHI of Plaintiffs and the Class Members against any future data breaches by ACG.

210. Plaintiffs' claims are typical of Class Members' claims in that Plaintiffs' claims and Class Members' claims all arise from ACG's failure to properly secure, safeguard and protect Plaintiffs' and Class Members' PII/PHI and the resulting Data Breach.

211. Plaintiffs and their counsel will fairly and adequately represent the interests of Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiffs' lawyers are experienced class action litigators and intend to vigorously prosecute this action on behalf of Plaintiffs and Class Members.

212. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and Class Members' claims. Plaintiffs and Class Members have been

irreparably harmed as a result of ACG's wrongful actions and/or inactions. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to ACG's failure to secure, safeguard and protect Plaintiffs' and Class Members' PII/PHI.

213. Class certification, therefore, is appropriate pursuant to Ala. R. Civ. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

214. Class certification also is appropriate pursuant to Ala. R. Civ. P. 23(b)(2) because ACG has acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the putative class as a whole.

215. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE/WANTONNESS
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

216. Plaintiffs incorporate by reference paragraphs 1-215 as if fully set forth herein.

217. ACG knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

218. ACG knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. ACG was

on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

219. ACG owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. ACG's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to federal and state law, HIPAA, and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

220. ACG's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 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.

221. ACG's duty also arose because Defendant was bound by industry standards to protect its patients' confidential Private Information.

222. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and ACG owed them a duty of care to not subject them to an unreasonable risk of harm.

223. ACG, through its actions and/or omissions, negligently and/or wantonly breached its duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within ACG's possession.

224. ACG, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

225. ACG, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

226. ACG breached its duties, and thus was negligent and/or wanton, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

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

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

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

e. Failing to comply with federal and state law, including HIPPA and the FTCA;

227. ACG had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust ACG with their Private Information was predicated on the understanding that ACG would take adequate security precautions. Moreover, only ACG had the ability to protect its systems (and the Private Information that it stored on them) from attack.

228. ACG's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

229. As a result of ACG's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

230. ACG's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

231. As a result of ACG's negligent and/or wanton conduct in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

232. ACG also had independent duties under federal and state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

233. As a direct and proximate result of ACG's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

234. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

235. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

236. Plaintiffs and the Class Members have suffered (and continue to suffer) actual, injuries-in-fact, and damages as a direct and/or proximate result of ACG's failure to secure, safeguard and protect their PII/PHI in the form of, inter alia, (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress—for which they are entitled to compensation.

237. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring ACG to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

238. Plaintiffs incorporate by reference paragraphs 1-215 as if fully set forth herein.

239. Federal and state statutory law and applicable regulations, including HIPAA's Privacy Rule, Section 5 of the Federal Trade Commission Act (15 U.S.C. §45), and the Alabama Data Breach Notification Act of 2018, set forth and otherwise establish duties in the industry that were applicable to ACG and with which ACG was obligated to comply at all relevant times hereto.

240. ACG violated these duties by failing to secure, safeguard and protect the Plaintiffs'

and Class Members' PII/PHI, which resulted in an unauthorized disclosure of the Plaintiffs' and the Class Members' PII/PHI.

241. Pursuant to Section 5 of the FTCA, ACG had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

242. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., ACG had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

243. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

244. Additionally, ACG violated its duty under Subsection 8-38-3(a) of the Alabama Data Breach Notification Act of 2018 which imposes a clear duty on entities like ACG to protect PII/PHI: "Each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security." (emphasis added).

245. ACG breached this duty owed to Plaintiff and the Class members under Subsection 8-38-3(a) of the Alabama Data Breach Notification Act of 2018 by failing to implement and maintain reasonable security measures to protect their sensitive PII and PHI against a breach of security.

246. ACG also breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

247. Specifically, ACG breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with HIPAA and the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

248. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of ACG's duty in this regard.

249. ACG also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

250. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to ACG's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

251. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and ACG's failure to comply with both constitutes negligence *per se*.

252. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to ACG's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

253. As a direct and proximate result of ACG's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

145. As a direct and proximate result of ACG's negligent and/or wanton conduct, Plaintiffs and Class Members have suffered injury and were damaged in the form of, without limitation, loss of time monitoring credit reports and financial accounts and placing credit freezes, expenses for credit monitoring and insurance, expenses for periodic credit reports, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm, and are entitled to compensatory and consequential damages in an amount to be proven at trial.

254. The harm suffered and that may be suffered in the future by the Plaintiffs and Class Members is the same type of harm HIPAA's Privacy Rule, the FTC Act and the Alabama Data Breach Notification Act of 2018 were intended to guard against.

255. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring ACG to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

256. Plaintiffs incorporate by reference paragraphs 1-215 as if fully set forth herein.

257. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to ACG in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

258. ACG's Privacy Policy memorialized the rights and obligations of ACG and its patients. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

259. In the Privacy Policy, ACG commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

260. Plaintiffs and Class Members fully performed their obligations under their contracts with ACG.

261. However, ACG did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore ACG breached its contracts with Plaintiffs and Class Members.

262. ACG allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, ACG breached the Privacy Policy with Plaintiffs and Class Members.

263. ACG's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in ACG providing services to Plaintiffs and Class Members that were of a diminished value.

264. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

265. As a direct and proximate result of ACG's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

266. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring ACG to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

267. Plaintiffs incorporate by reference paragraphs 1-215 as if fully set forth herein.

268. This Count is pleaded in the alternative to Count III above.

269. ACG provides cardiovascular health services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services and/or entrusting their valuable Private Information to Defendant in exchange for such services.

270. Through Defendant's sale of services to Plaintiffs and Class Members, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with its policies, practices, and applicable law.

271. As consideration, Plaintiffs and Class Members paid money to ACG and/or turned over valuable Private Information to ACG. Accordingly, Plaintiffs and Class Members bargained with ACG to securely maintain and store their Private Information.

272. ACG accepted payment and/or possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

273. In paying Defendant and/or providing their valuable Private Information to Defendant in exchange for Defendant's services, Plaintiffs and Class Members intended and understood that ACG would adequately safeguard the Private Information as part of those services.

274. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

275. Plaintiffs and Class Members would not have entrusted their Private Information to ACG in the absence of such an implied contract.

276. Had ACG disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to ACG.

277. As a provider of healthcare, ACG recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

278. ACG violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. ACG further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

279. Additionally, ACG breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

280. ACG also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

281. ACG further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

282. ACG further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

283. ACG further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

284. ACG further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

285. ACG further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

286. ACG further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

287. ACG further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

288. ACG further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

289. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide payment and/or accurate and complete Private Information to ACG in exchange for ACG's agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

290. Plaintiffs and Class Members have been damaged by ACG's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

291. Plaintiffs incorporate by reference paragraphs 1-215 as if fully set forth herein.

292. This Count is pleaded in the alternative to Counts III and IV above.

293. Plaintiffs and Class Members conferred a monetary benefit on ACG by turning over their Private Information to Defendant and by paying for healthcare services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

294. Upon information and belief, ACG funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

295. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal laws and regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to ACG.

296. ACG has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

297. ACG knew that Plaintiffs and Class Members conferred a benefit upon it, which ACG accepted. ACG profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for

adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

298. If Plaintiffs and Class Members had known that ACG had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

299. Due to ACG's conduct alleged herein, it would be unjust and inequitable under the circumstances for ACG to be permitted to retain the benefit of its wrongful conduct.

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

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

302. Plaintiffs and Class Members may not have an adequate remedy at law against ACG, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

303. Plaintiffs incorporate by reference paragraphs 1-215 as if fully set forth herein.

304. In light of the special relationship between ACG and its patients, whereby ACG became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) ACG was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members. This benefit included (1) the safeguarding of Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where ACG's patients' Private Information was and is stored.

305. ACG had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its patients' relationship, in particular to keep the Private Information secure.

306. ACG breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

307. ACG breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI ACG created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

308. ACG breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

309. ACG breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

310. ACG breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

311. ACG breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

312. ACG breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

313. ACG breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

314. ACG breached its fiduciary duty when it violated 45 C.F.R. § 164.530(b), and 45 C.F.R. § 164.308(a)(5) by failing to ensure that its workforce complied with HIPAA and failing to provide adequate training to their workforce.

315. ACG breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

146. ACG breached its fiduciary duty when it violated 45 C.F.R. § 164.530(c) by failing to design, implement, and enforce policies and procedures to establish a physical administrative safeguard to protect private information, such as PII/PHI.

147. Plaintiffs and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as a direct and proximate result of ACG's breaches of its fiduciary duties. These injuries include, but are not limited to:

a. Loss of control over private information;

b. Compromise of private information;

c. Lost opportunity costs associated with time spent to protect themselves and mitigating harm;

d. Continued risk that Plaintiff and Class Members private information could be stolen again;

e. Future costs associated with time spent protecting themselves from future harm;

f. Diminished value of ACG's services;

g. Diminished value of private information; and

h. Anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

316. Plaintiffs re-adopt and re-allege the factual allegations contained in the preceding paragraphs, and further allege as follows.

317. **DAMAGES**. As a direct and/or proximate result of ACG's wrongful actions and/or inactions (as described above), Plaintiffs and Class Members suffered (and continue to suffer) damages in the form of, inter alia: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure, dissemination and publication of their PII/PHI; (iii) criminal misuse of their PII/PHI; (iv) loss of privacy; (v) suspected and/or actual identity theft /financial fraud; (vi) out-of-pocket expenses incurred to mitigate the identity theft and financial fraud and the continued increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (vii) economic losses relating to the theft of their PII/PHI; (viii) the value of their time spent mitigating suspected and/or actual identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (ix) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (x) stress, anxiety and emotional distress. Plaintiffs' and Class Members' damages were foreseeable by ACG.

318. **EXEMPLARY DAMAGES**. Plaintiffs and Class Members also are entitled to exemplary damages to punish ACG and to deter such wrongful conduct in the future.

319. **INJUNCTIVE RELIEF**. Plaintiffs and Class Members also are entitled to injunctive relief in the form of, without limitation, requiring ACG to, inter alia, (i) immediately disclose to Plaintiffs and Class Members the precise nature and all details known to ACG regarding

the Data Breach, (ii) immediately secure the PII/PHI of its past, present, and future patients, (iii) implement the above-referenced proactive policies and procedures in order to secure and protect its patients' PII/PHI and be in a position to immediately notify them about any future data breaches, (iv) submit to periodic compliance audits by a third party regarding the implementation of and compliance with such policies and procedures, (v) submit to periodic compliance audits by a third party regarding the security of its patients' PII/PHI within its possession, custody and control, (vi) implement training for its personnel on new or modified security procedures through education programs, policies and tests, and (vii) pay for, not less than three years, identity theft and credit monitoring services for Plaintiffs and Class Members. Plaintiffs have standing to pursue injunctive relief. See Ala. Const. of 2022, art. I, section 10. ("That no person shall be barred from prosecuting or defending before any tribunal in this state, by himself or counsel, any civil cause to which he is a party.")

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, respectfully request that (i) ACG be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiffs be designated the Class Representatives, and (iv) Plaintiffs' counsel be appointed as Class Counsel. Plaintiffs, on behalf of themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against ACG, in favor of Plaintiffs and the Class Members, for:

i. actual damages, consequential damages, and/or nominal damages (as described above) in an amount to be determined by the trier of fact;

ii. exemplary damages;

iii. injunctive relief as set forth above;

iv. pre- and post-judgment interest at the highest applicable legal rates; costs of suit and attorneys' fees; and,

v. such other and further relief that this Court deems just and proper.

JURY DEMAND

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

Dated: December 30, 2024

Respectfully submitted,

/s/ Jon Mann

Jonathan S. Mann (MAN057)
PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Telephone: (205) 322-8880
E-mail: jonm@pittmandutton.com

Raina Borrelli (admitted *pro hac vice*)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
E-mail: raina@straussborrelli.com

Tyler J. Bean (admitted *pro hac vice*)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
E-mail: tbean@sirillp.com

Interim Co-Lead Class Counsel

Hunter Phares (PHA007)
CORY WATSON, P.C.
2131 Magnolia Avenue South
Birmingham, AL 35205
Telephone: (205) 328-2200
E-mail: hphares@corywatson.com

Interim Liasion Class Counsel

CERTIFICATE OF SERVICE

I hereby certify that on December 30, 2024, I filed the foregoing with the Clerk of the Court using the Court's AlaFile system, which will send notice to all counsel of record.

/s/ Jon Mann
Of Counsel

EXHIBIT A

Alabama Cardiovascular Group
AN AFFILIATE OF GRANDVIEW HEALTH

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 2, 2024

L7783-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

RE: Important Security Notification. Please read this entire letter.

Dear Sample A. Sample:

I'm writing on behalf of Alabama Cardiovascular Group ("ACG"). We sincerely regret to report that ACG experienced a security incident in which unauthorized parties accessed personal information in the ACG network. You are receiving this letter as a current or past patient of a physician at ACG, or a current or past patient guarantor, employee, or physician at ACG, whose personal information may have been affected.

We are committed to protecting personal information and sincerely regret any issues this incident may cause. We are offering identity theft protection for all affected individuals.

What happened? On July 2, 2024, ACG became aware that unauthorized parties accessed the ACG computer network. ACG disconnected the ACG computer network from the internet and cut off the unauthorized access. To protect against an incident like this from reoccurring, ACG reset user passwords and implemented additional security measures.

ACG's investigation determined that between June 6, 2024 and July 2, 2024, unauthorized parties gained access to the ACG network and obtained personal information. ACG has been in contact with law enforcement.

What personal information was involved? The personal information that may have been accessed varied from person to person. It may have included your name, address, email, phone number, demographic information such as date of birth, social security number, health insurance information and health insurance claims information, usernames and passwords, and medical information (such as dates of service, diagnoses, medications, images, lab results, and other treatment information). The personal information may also have included driver's license or passport numbers, credit card or debit card information, and bank account information if you had provided that type of information to ACG.

What are we doing? To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 24 months. A credit card is not required for enrollment in Experian IdentityWorks. To start monitoring your personal information:

- Ensure that you **enroll by November 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/plus.
- Provide your **activation code**: **KD4ZDW4TG8**

0000001

You will have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please contact an Experian agent. After it is determined that identity restoration support is needed, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

If you have further questions or concerns, or have questions about Experian IdentityWorks, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **866-720-0894** toll-free Monday through Friday 8 am – 8 pm CST, closed Saturday and Sunday (excluding major U.S. holidays) by November 30, 2024. Be prepared to provide engagement number **B126670** as proof of eligibility for the Identity Restoration services by Experian.

We are committed to the privacy of your personal information, and we sincerely regret the stress and worry this situation may cause you.

Sincerely,

Doranda Coker, Practice Administrator
Alabama Cardiovascular Group

What else can you do to protect your personal information?
We recommend you remain vigilant and consider taking the following steps:

Order your free credit report at annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about FCRA rights, see https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Place a fraud alert on your credit file. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a security freeze on your credit file, which generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. Contact the credit bureaus below to learn more about these or to place a fraud alert or request a security freeze on your account. The credit bureaus may require that you provide proper identification prior to honoring your request.

- **Equifax®**
  P.O. Box 740256
  Atlanta, GA 30374
  1-800-525-6285
  www.equifax.com
- **Experian®**
  P.O. Box 9554
  Allen, TX 75013
  1-888-397-3742
  www.experian.com
- **TransUnion®**
  P.O. Box 2000
  Chester, PA 19016
  1-800-680-7289
  www.transunion.com

Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

If you aren't already doing so, please ***pay close attention to all bills and credit card charges*** to check for items you did not contract for or purchase. ***Review all your bank account statements*** frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

Change your passwords. ACG reset passwords for ACG accounts. However, if you use the same usernames and/or passwords across different sites, we recommend that you promptly change them.

Where can I get additional information? The FTC offers consumer assistance and educational materials relating to identity theft and privacy issues. You can learn more about how to protect yourself from becoming an identity theft victim, including fraud alerts and security freezes, by contacting the FTC at 877.IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

You may also contact your state's Attorney General to obtain information about fraud alerts and security freezes, security breaches, and how to prevent identity theft. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the FTC. You may also obtain a copy of police reports.

For District of Columbia Residents: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202.727.3400, oag.dc.gov.

For Maryland Residents: Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888.743.0023, https://www.marylandattorneygeneral.gov/.

For New York Residents: New York Attorney General, 212-416-8433 or https://ag.ny.gov/internet/resource-center. NYS Department of State's Division of Consumer Protection, 800-697-1220 or https://dos.ny.gov/consumer-protection.

For North Carolina Residents: North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, ncdoj.gov.

For Rhode Island Residents: Rhode Island Attorney General's Office, 150 South Main Street Providence, RI 02903; Phone: 401-274-4400; Website: www.riag.ri.gov

ACG is a dba of Affinity Cardiovascular Specialists, LLC, and an affiliate of Birmingham Holdings, LLC

Alabama Cardiovascular Group
AN AFFILIATE OF GRANDVIEW HEALTH

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 2, 2024

L7783-L02-0000002 T00001 P001 ********SCH 5-DIGIT 12345
PARENT OR GUARDIAN OF
SAMPLE A SAMPLE - L02 MINOR
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

RE: Important Security Notification. Please read this entire letter.

Dear Parent or Guardian of Sample A. Sample:

I'm writing on behalf of Alabama Cardiovascular Group ("ACG"). We sincerely regret to report that ACG experienced a security incident in which unauthorized parties accessed personal information in the ACG network. You are receiving this letter as a parent or guardian of a minor dependent who is a past or present patient of ACG. Your dependent's personal information, or your personal information as a guarantor, may have been affected.

We are committed to protecting personal information and sincerely regret any issues this incident may cause. We are offering identity theft protection for all affected individuals.

What happened? On July 2, 2024, ACG became aware that unauthorized parties accessed the ACG computer network. ACG disconnected the ACG computer network from the internet and cut off the unauthorized access. To protect against an incident like this from reoccurring, ACG reset user passwords and implemented additional security measures.

ACG's investigation determined that between June 6, 2024 and July 2, 2024, unauthorized parties gained access to the ACG network and obtained personal information. ACG has been in contact with law enforcement.

What personal information was involved? The personal information that may have been accessed varied from person to person. It may have included name, address, email, phone number, demographic information such as date of birth, social security number, health insurance information and health insurance claims information, usernames and passwords, and medical information (such as dates of service, diagnoses, medications, images, lab results, and other treatment information). The personal information may also have included driver's license or passport numbers, credit card or debit card information, and bank account information if you had provided that type of information to ACG.

What we are doing. To help protect yours and your minor dependent's identity, we are offering complimentary access to Experian IdentityWorks℠ for 24 months. A credit card is not required for enrollment in Experian IdentityWorks. There are different instructions and activation codes for adults and minors below:

Minor Enrollees:

- Ensure that you **enroll by November 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/minorplus
- Provide your **activation code**: **G24F4NP85T**
- Provide the **engagement number: B126675**

You will have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Adult/Guarantor Enrollees:

- Ensure that you **enroll by November 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/plus.
- Provide your **activation code**: **KD4ZDW4TG8**
- Provide the **engagement number: B126670**

You will have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please contact an Experian agent. After it is determined that identity restoration support is needed, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

If you have further questions or concerns, or if you have questions about Experian IdentityWorks, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **866-720-0894** toll-free Monday through Friday 8 am – 8 pm CST, closed Saturday and Sunday (excluding major U.S. holidays) by November 30, 2024. Be prepared to provide the engagement number above as proof of eligibility for the Identity Restoration services by Experian.

We are committed to the privacy of your personal information, and we sincerely regret the stress and worry this situation may cause you.

Sincerely,

Doranda Coker, Practice Administrator
Alabama Cardiovascular Group

What else can you do to protect your personal information?
We recommend you remain vigilant and consider taking the following steps:

Order your free credit report at annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about FCRA rights, see https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Place a fraud alert on your credit file. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a security freeze on your credit file, which generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. Contact the credit bureaus below to learn more about these or to place a fraud alert or request a security freeze on your account. The credit bureaus may require that you provide proper identification prior to honoring your request.

- **Equifax®**
  P.O. Box 740256
  Atlanta, GA 30374
  1-800-525-6285
  www.equifax.com

- **Experian®**
  P.O. Box 9554
  Allen, TX 75013
  1-888-397-3742
  www.experian.com
- **TransUnion®**
  P.O. Box 2000
  Chester, PA 19016
  1-800-680-7289
  www.transunion.com

Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

If you aren't already doing so, please ***pay close attention to all bills and credit card charges*** to check for items you did not contract for or purchase. ***Review all your bank account statements*** frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

Change your passwords. ACG reset passwords for ACG accounts. However, if you use the same usernames and/or passwords across different sites, we recommend that you promptly change them.

Where can I get additional information? The FTC offers consumer assistance and educational materials relating to identity theft and privacy issues. You can learn more about how to protect yourself from becoming an identity theft victim, including fraud alerts and security freezes, by contacting the FTC at 877.IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

You may also contact your state's Attorney General to obtain information about fraud alerts and security freezes, security breaches, and how to prevent identity theft. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the FTC. You may also obtain a copy of police reports.

For District of Columbia Residents: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202.727.3400, oag.dc.gov.

For Maryland Residents: Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888.743.0023, https://www.marylandattorneygeneral.gov/.

For New York Residents: New York Attorney General, 212-416-8433 or https://ag.ny.gov/internet/resource-center. NYS Department of State's Division of Consumer Protection, 800-697-1220 or https://dos.ny.gov/consumer-protection.

For North Carolina Residents: North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, ncdoj.gov.

For Rhode Island Residents: Rhode Island Attorney General's Office, 150 South Main Street Providence, RI 02903; Phone: 401-274-4400; Website: www.riag.ri.gov

ACG is a dba of Affinity Cardiovascular Specialists, LLC, and an affiliate of Birmingham Holdings, LLC.

Alabama Cardiovascular Group
AN AFFILIATE OF GRANDVIEW HEALTH

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 2, 2024

L7783-L03-0000002 T00001 P001 ********SCH 5-DIGIT 12345
TO THE ESTATE OF
SAMPLE A SAMPLE - L03 DECEASED
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

RE: Important Security Notification. Please read this entire letter.

To the Next of Kin/Estate of Sample A. Sample:

I'm writing on behalf of Alabama Cardiovascular Group ("ACG"). We sincerely regret to report that ACG experienced a security incident in which unauthorized parties accessed personal information in the ACG network. You are receiving this letter on behalf of the decedent who was a former patient of ACG, whose personal information may have been affected.

We are committed to protecting personal information and sincerely regret any issues this incident may cause.

What happened? On July 2, 2024, ACG became aware that unauthorized parties accessed the ACG computer network. ACG disconnected the ACG computer network from the internet and cut off the unauthorized access. To protect against an incident like this from reoccurring, ACG reset user passwords and implemented additional security measures.

ACG's investigation determined that between June 6, 2024 and July 2, 2024, unauthorized parties gained access to the ACG network and obtained personal information. ACG has been in contact with law enforcement.

What personal information was involved? The personal information that may have been accessed varied from person to person. It may have included name, address, email, phone number, demographic information such as date of birth, social security number, health insurance information and health insurance claims information, usernames and passwords, and medical information (such as dates of service, diagnoses, medications, images, lab results, and other treatment information). The personal information may also have included driver's license or passport numbers, credit card or debit card information, and bank account information if you had provided that type of information to ACG.

What can you do? This notice including the attached sheet provides precautionary measures you can take to protect the decedent's personal information, including contacting one of the nationwide credit bureaus to notify them of the decedent's death which will cause a death notice to be placed on their credit reports. A death notice flags a person's credit reports as "deceased - do not issue credit." Additionally, you should always remain vigilant in reviewing the decedent's financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

If you have questions or concerns related to this incident, ACG has established a toll-free response line that can be reached at **866-720-0894**, and is available Monday through Friday 8 am – 8 pm CST, closed Saturday and Sunday (excluding major U.S. holidays). Be prepared to provide engagement number **B126671**.

We are committed to protecting personal information, and we sincerely regret the stress and worry this situation may cause you.

Sincerely,

Doranda Coker, Practice Administrator
Alabama Cardiovascular Group

What else can you do to protect the decedent's personal information?

We recommend you remain vigilant and consider taking the following steps:

Order a free credit report at annualcreditreport.com, call toll-free at 877.322.8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov. When you receive the decedent's credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in the decedent's name (credit granters, collection agencies, etc.) so that you can follow through with these entities. For more information about FCRA rights, see https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Place a fraud alert. If you have not already done so, you can also request the three credit bureaus to place the following alert in the decedent's file:

> **"**Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

Here is the contact information for the three credit bureaus:

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016-2000
800-525-6285	888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Remove the decedent's name from mailing lists of pre-approved offers of credit.

Pay close attention to all bills and credit card charges you receive and check for items the decedent did not purchase. ***Review all bank account statements*** frequently for checks, purchases, or deductions not made by the decedent or you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically because identity thieves sometimes hold on to stolen personal information before using it.

Change your passwords. ACG reset passwords for ACG accounts. However, if you use the same usernames and/or passwords across different sites, we recommend that you promptly change them.

Where can I get additional information? The FTC offers consumer assistance and educational materials relating to identity theft and privacy issues. You can learn more about how to protect yourself from becoming an identity theft victim, including fraud alerts and security freezes, by contacting the FTC at 877.IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

You may also contact your state's Attorney General to obtain information about fraud alerts and security freezes, security breaches, and how to prevent identity theft. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the FTC. You may also obtain a copy of police reports.

For District of Columbia Residents: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202.727.3400, oag.dc.gov.

For Maryland Residents: Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888.743.0023, https://www.marylandattorneygeneral.gov/.

For New York Residents: New York Attorney General, 212-416-8433 or https://ag.ny.gov/internet/resource-center. NYS Department of State's Division of Consumer Protection, 800-697-1220 or https://dos.ny.gov/consumer-protection.

For North Carolina Residents: North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, ncdoj.gov.

For Rhode Island Residents: Rhode Island Attorney General's Office, 150 South Main Street Providence, RI 02903; Phone: 401-274-4400; Website: www.riag.ri.gov

ACG is a dba of Affinity Cardiovascular Specialists, LLC, and an affiliate of Birmingham Holdings, LLC.