Exhibit C22

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA
COLUMBUS DIVISION

ERIN THERESA GRAY, on behalf of herself and all others similarly situated,	*	
	*	**Civil Action Case No:**
Plaintiffs,	*	
v.	*	_____
	*	
LABORATORY CORPORATION OF AMERICA HOLDINGS, QUEST DIAGNOSTICS INCORPORATED, and OPTUM360, LLC,	*	**CLASS ACTION COMPLAINT & DEMAND FOR JURY TRIAL**
	*	
Defendants.	*	

Plaintiff, Erin Theresa Gray, ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following, against Defendants Laboratory Corporation of America Holdings ("LabCorp"), Quest Diagnostics Incorporated ("Quest"), and Optum360 Services, Inc. ("Optum360. Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

SUMMARY OF THE CASE

1. Plaintiff brings this class action on behalf of a nationwide class against Defendants because of their failure to protect the confidential information of millions of patients—including financial information, medical information, and personally identifiable information ("PII"), and/or other protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Personal Sensitive Information"). Defendants' wrongful disclosure has harmed Plaintiff and the Class, which includes thousands of individuals.

2. LabCorp and Quest are two of the largest medical testing providers in the country.

They provide clinical diagnostic services to the public, doctors' offices, hospitals and clinics. In doing so, they collect private personal, medical, and financial information from their customers in providing services.

3. Plaintiff entrusted her Personal Sensitive Information to Defendants when they were retained for diagnostic services, expecting them to protect her Personal Sensitive Information.

4. After entrusting her Personal Sensitive Information with LabCorp and Quest, they shared the Personal Sensitive Information with third-party vendors, AMCA and Optum 360, billing collection service providers for LabCorp and Quest.

5. Between August 1, 2018 and March 30, 2019, AMCA's computer systems were hacked allowing unauthorized access to millions of records of patients of LabCorp and Quest, including Plaintiff (the "Data Breach").

6. On June 3, 2019, Quest announced that AMCA had informed Quest that "an unauthorized user had access to AMCA's system containing personal information AMCA received from various entities, including Quest."[1] Approximately 11.9 million Quest patients' Personal Sensitive Information was compromised in the Data Breach.

7. On June 4, 2019, LabCorp announced that it was also impacted by the Data Breach, and had previously "referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system", and that "AMCA has informed LabCorp that it is in the process of sending notices to approximately 200,000 LabCorp consumers whose credit card or

[1] Press Release, Quest Diagnostics Incorporated, "Quest Diagnostics Statement on the AMCA Data Security Incident" (June 3, 2019), *available at* http://newsroom.questdiagnostics.com/AMCADataSecurityIncident

bank account information may have been accessed."[2]

8. LabCorp and Quest breached their duties to patients across the country by providing patient information to third-party vendors that utilized remarkably inferior data security practices such that the intrusion remained undetected for almost eight months all the while patients' information was being placed for sale on the dark web.

9. The Data Breach was the direct result of the inadequate approach of LabCorp and Quest to data security and its failure to protect their patients' Personal Sensitive Information that Defendants collected and shared with AMCA and Optum360 in the normal course of business.

10. Now as a direct result of Defendants' failure to reasonably protect Personal Sensitive Information of the Plaintiff and the putative class, Plaintiff and the class members have incurred and will continue to incur significant damages in reducing the risk of identity theft and other fraudulent activity.

11. Plaintiff, on behalf of herself and similarly situated individuals, seeks to recover damages (compensatory and reimbursement of costs that they have had to incur), equitable relief, and injunctive relief that would require Defendants to implement industry-standard data security and data-sharing practices to protect PII and PHI so another data breach does not occur.

PARTIES

12. At all times relevant, Plaintiff has been a Harris County, Georgia resident when her Personal Sensitive Information was compromised in the Data Breach described herein. Plaintiff used LabCorp and sometimes Quest for diagnostic services. On information and belief, Plaintiffs Personal Sensitive Information was compromised in the Data Breach, and because of Defendants'

[2] Form 8-K, Laboratory Corporation of America Holdings, filed June 4, 3019, *available at* https://www.sec.gov/Archives/edgar/data/920148/000119312519165091/d757830d8k.htm

failures to prevent the Data Breach, she will be at an increased risk for fraud, identity theft, and any related consequent damages.

13. Defendant Laboratory Corporation of America Holdings ("LabCorp") is a corporation organized under the laws of Delaware and has its principal place of business at 358 South Main Street, Burlington, North Carolina 27215.

14. Defendant Quest Diagnostics Incorporated ("Quest") is a Delaware corporation and has its principal place of business at 500 Plaza Drive, Secaucus, New Jersey 07094.

15. Defendant Optum360, LLC ("Optum360") is a Delaware limited liability company and is headquartered at 13625 Technology Drive, Eden Prairie, Minnesota 55344.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because at least one member of the putative Class is a citizen of a state different from at least one Defendant, there are more than 100 putative class members, and the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

17. This Court has personal jurisdiction over Defendants because Defendants do substantial business in and throughout Georgia, and a portion of the wrongful acts alleged herein were committed in Georgia, among other venues.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) because a substantial part of the events, acts, and omissions giving rise to the claims of the Plaintiff occurred in this district.

FACTUAL BACKGROUND

A. LabCorp and Quest Obtained Plaintiff's Personal Sensitive Information and Shared it with their Vendors.

19. LabCorp is a leading global life sciences company that "provides diagnostic, drug development and technology-enabled solutions for more than 120 million patient encounters per year [and] processes tests on more than 2.5 million patient specimens per week". [3]

20. Quest is one of the world's leading provider of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease. Quest collects personal, medical and financial information from its customers in providing its services.

21. AMCA is LabCorp's billing collection vendor. Quest also relies on AMCA for its billing collection services. AMCA, according to its website, is "the leading Patient recovery agency" and is "one of the nation's top agencies managing over $1BN in annual receivables."[4] The AMCA has consistently received negative reviews from consumers, including receiving an "F" rating from the Better Business Bureau.[5] The Consumer Financial Protection Bureau ("CFPB") has received nearly 700 consumer complaints against the AMCA since 2013.[6]

22. Optum360 is Quest's revenue cycle management provider.

23. LabCorp and Quest collect, store and maintain extensive amounts of highly sensitive protected health information and other personally identifiable information of patients who use LabCorp or Quest for diagnostic and laboratory services. LabCorp and Quest routinely

---

[3] Form 10-K, p. 4; http://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_LH_2018.pdf
[4] AMCA, *About Us*, available at http://amcaonline.com/ (last visited June 18, 2019).
[5] Better Business Bureau, *American Medical Collection Agency*, available at https://www.bbb.org/us/md/baltimore/profile/collections-agencies/american-medical-collection-bureau-0011-90192010 (last visited June 18, 2019).
[6] CFPB Consumer Complaint Database, *Retrieval Masters*, available at https://www.consumerfinance.gov/data-research/consumer-complaints/search/?from=0&searchField=all&searchText=Retrieval%20Masters&size=25&sort=created_date_desc (last visited June 18, 2019).

share this Personal Sensitive Information with their vendors, e.g., AMCA.

24. LabCorp and Quest charge for laboratory services provided to patients. The invoices sent are for laboratory testing fees which are separate from bills patients receive from their doctors. Patients whose insurance does not cover the services and uninsured patients are responsible for payment.

25. When a LabCorp invoice is unpaid within the requested time period, it sends the invoice to a collection agency. AMCA provides billing collections services to LabCorp.

26. When a Quest invoice is unpaid within the requested time period, it sends the invoice to a collection agency. Quest partners with Optum360 for billing and collection processes. AMCA provides billing collections service to Optum360.

27. Upon information and belief, LabCorp and Quest, provided AMCA with Personal Sensitive Information about patients, including Plaintiff and the putative Class, in order to facilitate the bill collection process.

28. The patient information LabCorp and Quest provided to AMCA contained Personal Sensitive Information that included personal and medical information, such as the first and last name, date of birth, address, phone, date of service, service provider, and account balance information, and social security numbers.

29. Upon information and belief, AMCA stored the information LabCorp and Quest provided to AMCA in its own computer systems. These same AMCA systems were compromised in the Data Breach.

B. Defendants Owed a Duty to Protect Plaintiff's and the Class' Personal Sensitive Information.

30. Defendants had a duty, obligation, and agreed to keep confidential the Personal

Sensitive Information their patients disclosed to them and to protect this information from unauthorized disclosure. Defendants' agreement, duties, and obligations are based on: (1) HIPAA; (2) industry standards; and (3) the agreements and promises made to Plaintiff and the putative Classes. Class members provided their Personal Sensitive Information to Defendants with the reasonable belief that Defendants and their business affiliates would comply with their agreements and any legal requirements to keep that Personal Sensitive Information confidential and secure from unauthorized disclosure.

31. Defendants have a well-established and clear legal duty to act reasonably to protect patients' Personal Sensitive Information that they collect and possess from exposure to unauthorized third parties.

32. When Plaintiffs and the Class provided Defendants with their most sensitive information, or when Defendants received such information in some other manner, Plaintiffs and the Class reasonably expected that such information would be stored by Defendants in safe and confidential manner, using all reasonable safeguards and protections.

33. Defendants had obligations, arising from promises made to patients like Plaintiff and Class Members, and based on industry standards, to keep the compromised Personal Sensitive Information confidential and to protect it from unauthorized disclosure.

C. The Data Breach

34. On June 3, 2019, Quest publicly announced in a periodic public filing Form 8-K and an accompanying press release that highly sensitive information of 11.9 million of its patients had been improperly exposed over a period of 7 months. The breach occurred on the systems of Quest's billing collections vendor, AMCA. The filing states, "between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that

AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself." The release further provided that a broad array of sensitive information was exposed such as "financial information (e.g., credit cards and bank account information), medical information and other personal information (e.g., Social Security Numbers)." As announced by Quest on June 3, 2019:

> Quest Diagnostics Statement on the AMCA Data Security Incident
>
> SECAUCUS, N.J., June 03, 2019: American Medical Collection Agency (ACMA), a billing collections service provider, has informed Quest Diagnostics that an unauthorized user had access to AMCA's system containing personal information AMCA received from various entities, including from Quest. AMCA provides billing collections services to Optum360, which in turn is a Quest contractor, Quest and Optum360 are working with forensic experts to investigate the matter.
>
> AMCA first notified Quest and Optum360 on May 14, 2019, of potential unauthorized activity on AMCA's web payment page. On May 31, 2019, AMCA notified Quest and Optum360 that the data on AMCA's affected system included information regarding approximately 11.9 million Quest patients. AMCA believes this information includes personal information, including certain financial data, Social Security numbers, and medical information, but not laboratory test results.
>
> AMCA has not yet provided Quest or Optum360 detailed or complete information about the AMCA data security incident, including which information of which individuals may have been affected. Quest has not been able to verify the accuracy of the information received from AMCA.
>
> Quest is taking this matter very seriously and is committed to the privacy and security of our patients' personal information. Since learning of the AMCA data security incident, we have suspended sending collection requests to AMCA.
>
> Quest will be working with Optum360 to ensure that Quest patients are appropriately notified consistent with the law.
>
> We are committed to keeping our patients, health care providers, and all

relevant parties informed as we learn more.[7]

35. On June 4, 2019, LabCorp announced through a securities filing that it had been impacted by the Data Breach as well. LabCorp's Form 8-K filing disclosed, in relevant part:

> According to AMCA, [the Data Breach] occurred between August 1, 2018, and March 30, 2019. AMCA is an external collection agency used by LabCorp and other healthcare companies. LabCorp has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system. AMCA's affected system included information provided by LabCorp. That information could include first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA's affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance). LabCorp provided no ordered test, laboratory results, or diagnostic information to AMCA. AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp consumers.
>
> AMCA has informed LabCorp that it is in the process of sending notices to approximately 200,000 LabCorp consumers whose credit card or bank account information may have been accessed. AMCA has not yet provided LabCorp a list of the affected LabCorp consumers or more specific information about them.[8]

36. Defendants had obligations created by HIPAA, arising from promises made to patients like Plaintiff and other Class Members, and based on industry standards, to keep the compromised Personal Sensitive Information confidential and to protect it from unauthorized disclosures. Class Members provided their Personal Sensitive Information to LabCorp and Quest with the understanding that they and any business partners to whom they disclosed the Personal Sensitive Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

---

[7] June 03, 2019 Press release, *Quest Diagnostics Statement on the AMCA Data Security Incident, available at* http://newsroom.questdiagnostics.com/AMCADataSecurityIncident (last visited July 24, 2019).

[8] Form 8-K, Laboratory Corporation of America Holdings, filed June 4, 3019, *available at* https://www.sec.gov/Archives/edgar/data/920148/000119312519165091/d757830d8k.htm

37. LabCorp was aware of its obligations and duties to protect its patients' Personal Sensitive Information, as evidenced by LabCorp's Notice of Privacy Practices:

> Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), LabCorp is required by law to maintain the privacy of health information that identifies you, called protected health information (PHI), and to provide you with notice of our legal duties and privacy practices regarding PHI. LabCorp is committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation. We take this commitment seriously and will work with you to comply with your right to receive certain information under HIPAA.[9]

38. LabCorp also understood that it was required under HIPAA, as well as other state and federal laws, to implement adequate security measures to protect Personal Sensitive Information:

> The Company has implemented policies and procedures designed to comply with the HIPAA privacy and security requirements as applicable. The privacy and security regulations establish a "floor" and do not supersede state laws that are more stringent. Therefore, the Company is required to comply with both additional federal privacy and security regulations and varying state privacy and security laws. In addition, federal and state laws that protect the privacy and security of patient information may be subject to enforcement and interpretations by various governmental authorities and courts, resulting in complex compliance issues. For example, the Company could incur damages under state laws pursuant to an action brought by a private party for the wrongful use or disclosure of health information or other personal information.[10]

39. LabCorp was further aware of the risks and consequences for failing to maintain adequate data security systems and practices, as well as the same risks and consequences for its vendors and subcontractors:

> Failure to maintain the security of customer-related information or compliance with security requirements could damage the Company's

[9] LabCorp, "HIPAA Notice of Privacy Practices", *available at* https://www.labcorp.com/hipaa-privacy/hipaa-information (last accessed June 25, 2019).
[10] Form 10-K at 3, *supra* n. 8.

> reputation with customers, cause it to incur substantial additional costs and become subject to litigation and enforcement actions.
>
> The Company receives and stores certain personal and financial information about its customers. In addition, the Company depends upon the secure transmission of confidential information over public networks, including information permitting cashless payments. The Company also works with third-party service providers and vendors that provide technology systems and services that are used in connection with the receipt, storage and transmission of customer personal and financial information. A compromise in the Company's security systems, or those of the Company's third party service providers and vendors, that results in customer personal information being obtained by unauthorized persons or the Company's or third party's failure to comply with security requirements for financial transactions could adversely affect the Company's reputation with its customers and others, as well as the Company's results of operations, financial condition and liquidity. It could also result in litigation against the Company and the imposition of fines and penalties.[11]

40. LabCorp was also specifically aware of the dangers of data breaches and cyber-attacks, and the subsequent risks and harms that its patients would suffer if their Personal Sensitive Information was compromised:

> Security breaches and unauthorized access to the Company's or its customers' data could harm the Company's reputation and adversely affect its business.
>
> The Company has experienced and expects to continue to experience attempts by computer programmers and hackers to attack and penetrate the Company's layered security controls, like the 2018 ransomware attack. These attempts, if successful, could result in the misappropriation or compromise of personal information or proprietary or confidential information stored within the Company's systems, create system disruptions or cause shutdowns. External actors may be able to develop and deploy viruses, worms and other malicious software programs that attack the Company's systems or otherwise exploit any security vulnerabilities…. Breaches of the Company's security measures and the unauthorized dissemination of personal, proprietary or confidential information about the Company or its customers or other third-parties could expose customers' private information. Such breaches could expose customers to the risk of financial or medical identity theft or expose the Company or other third

[11] *Id.*

> parties to a risk of loss or misuse of this information, result in litigation and potential liability for the Company, damage the Company's brand and reputation or otherwise harm the Company's business. Any of these disruptions or breaches of security could have a material adverse effect on the Company's business, regulatory compliance, financial condition and results of operations.[12]

41. LabCorp was on notice of the risk of data breach because it was previously the target of a cyber-attack that compromised LabCorp's Systems:

> On July 16, 2018, the Company reported that it had detected suspicious activity on its information technology network and was taking steps to respond to and contain the activity. The activity was subsequently determined to be a new variant of ransomware affecting certain LCD information technology systems. In response, the Company took certain systems offline which temporarily affected test processing and customer access to test results, and also affected certain other information technology systems involved in conducting Company-wide operations. To date, the Company has not been the subject of any legal proceedings involving this incident, but it is possible that the Company could be the subject of claims from persons alleging they suffered damages from the incident, or actions by governmental authorities. The Company cooperated with law enforcement and regulatory authorities with respect to the incident. [13]

42. Likewise, Quest promises patients that it will keep their Personal Sensitive Information confidential, assuring patients that it is "committed to protecting the privacy of your identifiable health information." [14]

43. In its Notice of Privacy Practices, Quest acknowledges that it is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[15]

44. Quest informs patients: "We may provide your PHI [(Private Health Information)] to other companies or individuals that need the information to provide services to us. These other

[12] Form 10-K at 41.
[13] *Id.* at 48-49.
[14] *Quest* Diagnostics, *Notice of Privacy Practices*, http://questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html (last visited July 24, 2019).
[15] Id.

entities, known as 'business associates,' are required to maintain the privacy and security of PHI."[16]

45. Quest was on alert to the risk of a data breach. It suffered a data breach in November 2016 when an unauthorized third party accessed the Quest patient portal known as "MyQuest" and obtained the PHI of approximately 34,000 patients.[17]

46. Defendants' data security obligations and promises were particularly important given the substantial increase in data breaches -- particularly those in the healthcare industry (e.g., Anthem, Inc., Premera Blue Cross, Excellus Health Plan Inc.) -- preceding August 2018, which were widely known to the public and to anyone in Defendants' industries.

47. Defendants knew through personal experience that given the vast amount of PII they managed and maintained, having been a prior target of attempted cyber and other security threats, and thus understood the risks posed by their insecure data security practices and systems. They also understood the need to safeguard PII and the impact a data breach would have on their patients, including Plaintiff and the Class.

D. The Data Breach Harmed Plaintiff and Will Result in Additional Harm

48. Plaintiff and other Class Members have been injured by the disclosure of their Personal Sensitive Information in the Data Breach.

49. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in

[16] Id.
[17] Quest Diagnostics, *Quest Diagnostics Provides Notice of Data Security Incident* (Dec. 12, 2016), available at http://ir.questdiagnostics.com/node/13111/pdf (last visited June 18, 2019).

a person's name.[18] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

50. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[19]

51. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers ("SSNs") for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

52. There may be a time lag between when Sensitive Information is stolen and when it is used. According to the GAO Report:

> [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.[20]

53. With access to an individual's Personal Sensitive Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a

[18] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited July 24, 2019).
[19] *Id*. at 2, 9
[20] *Id*. at 29 (emphasis supplied).

fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[21]

54. Personal Sensitive Information 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 years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Personal Sensitive Information directly on various Internet websites making the information publicly available.

55. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[22]

56. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole. Medical databases are especially valuable to identity thieves. According to a 2012 nationwide insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[23] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

---

[21] *See Federal Trade Commission*, Warning Signs of Identify Theft, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited July 24, 2019).

[22] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, (Mar. 3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited July 24, 2019).

[23] *See* Study; Few Aware of Medical Identity Theft Risk, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited July 24, 2019).

E. Plaintiff and Class Members Are in Imminent Danger of Identity Theft.

57. Defendants caused harm to Plaintiff and putative Class members by sharing their Personal Sensitive Information with AMCA. LabCorp and Quest failed to properly monitor its vendor, and AMCA failed to prevent attackers from accessing and stealing this information in the Data Breach.

58. Hackers are known for stealing and selling Personal Sensitive Information in order to use it for illicit means and financial gain. The question is when, not whether, it will be misused. But whether or not the Personal Sensitive Information stolen in the Data Breach is later used in a criminal enterprise, Plaintiff and putative Class members suffered economic harm as just the theft of their Personal Sensitive Information increases the risk of their identity being exploited in ways that can cause economic harm to them. This increased risk decreases the value of their Personal Sensitive Information.

59. Plaintiff and members of the putative Classes have experienced fraud at or near the time of the announced Data Breach, including Plaintiff Gray.

F. Defendants Failed to Comply with HIPAA

60. Despite representations to the contrary, Defendants' security failures demonstrate that they failed to comply with HIPAA regulations and mandated safeguards. Title II of HIPAA (42 U.S.C. §§ 1301 et seq.) require the Department of Health and Human Services to establish standards and rules for how Personal Sensitive Information should be safeguarded. Defendants failed to comply with their duties under HIPAA. Defendants failed to:

i. Maintain adequate data security system to reduce the risk of data breaches and cyber-attacks;

ii. Properly ensure vendors and other third-parties entrusted with Personal Sensitive Information were employing proper data security practices that

would ensure the security of Plaintiff's and the Class' Personal Sensitive Information;

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

iv. 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 C.F.R. § 164.312(a)(1);

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

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

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

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

ix. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

x. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

xi. Design, implement, and enforce policies and procedures that establish physical and administrative safeguards for protected health information, pursuant to 45 C.F.R. § 164.530(c).

G. Defendants Failed to Comply with Requirements Established by The Federal Trade Commission

61. According to the Federal Trade Commission ("FTC"), the failure to employ

reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 (the "FTC Act"), 15 U.S.C. § 45.

62. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. 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 for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack 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.

63. The FTC also has published a document, entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

64. And the FTC has issued orders against businesses that failed to employ reasonable measures to secure data. These orders provide further guidance to businesses with regard to their data security obligations.

65. In the months and years leading up to the Data Breach, and during the course of the breach itself, Defendants failed to follow the guidelines recommended by the FTC. Further, by failing to have reasonable data security measures in place, Defendants engaged in unfair acts or practices within the meaning of Section 5 of the FTC Act.

H. Defendants Failed to Comply with Data Security Industry Standards.

66. In addition to the sensitive health and medical information that was compromised in the Data Breach, Defendants' permitted the theft of other sensitive PII, including credit card numbers and bank account information.

67. Defendants' had a duty of care to maintain the confidentiality of Plaintiffs and the Class members' credit card numbers and bank account information.

68. The Payment Card Industry Security Standards Council promulgates a set of minimum requirements, which apply to all organizations that store, process, or transmit Payment Card Data. This standard, known as the Payment Card Industry Data Security Standard ("PCI DSS"), is the industry standard governing the security of payment card data. It sets the minimum level of what must be done, not the maximum.

69. The Payment Card Industry Security Standards Council has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[24]

70. Gemini Advisory found credit card numbers from the breach for sale on the dark web, which means that AMCA did not encrypt those numbers in accordance with PCI DSS.

71. If AMCA had implemented a P2PE solution prior to the data breach and an

[24] Securing Account Data with the PCI Point –to-Point Encryption Standard v2, available at https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf

attacker were to steal encrypted payment card data, that data would have been commercially worthless to the attacker as the attacker would not be able to decrypt the data to obtain the information necessary to make fraudulent purchases.

72. PCI DSS v.3.2, in effect beginning April 2016, imposes mandates relating to maintaining a secure network and systems, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks and maintaining an information security policy. PCI DSS v.3.2 establishes comprehensive requirements that must be followed to meet these mandates.

73. PCI DSS required Defendants to properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; implement proper network segmentation; restrict access to Payment Card Data to those with a need to know; and establish a process to identify and timely fix security vulnerabilities.

74. Defendants failed to comply with the requirements of PCI DSS v.3.2.

CLASS ACTION ALLEGATIONS

75. Under the Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), Plaintiff brings forth this action on behalf of herself and seeks certification of a Nationwide Class defined as follows:

> All persons residing in the United States who used LabCorp and or Quest and provided PII to Lab Corp and /or Quest and whose Personal Sensitive Information was exposed to unauthorized third parties as a result of the Data Breach announced on June 3, 2019 and June 4, 2019. ("The Class").

76. Plaintiff reserves the right to amend or modify the class definition after conducting discovery.

CLASS ACTION CERTIFICATION REQUIREMENTS

77. As set forth in the Federal Rules of Civil Procedure 23(a), Plaintiff must establish the following elements to obtain class certification: (1) numerosity; (2) commonality; (3) typicality; and (4) the adequacy of representation.

78. Numerosity: As a result of Defendants' actions, Plaintiff was harmed as a result of a data breach that affected of millions of people nationwide. From a geographical standpoint, these individuals are dispersed across the country and are so numerous that joinder of individual claims would be impracticable. The class action procedure here will have no management difficulties. Defendants' records and the records available publicly will easily identify the Class Members.

79. Commonality: Questions of law and fact common to the claims of Plaintiff and the other members of the Classes predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include:

a. Whether Defendants had a duty to protect Personal Sensitive Information;

b. Whether Defendants knew or should have known that AMCA's systems were susceptible to a data breach;

c. Whether Defendants' storage of Plaintiff's and the Class' Personal Sensitive Information violated HIPPA, industry standards and federal law;

d. Whether Defendants negligently or otherwise improperly allowed Personal Sensitive Information to be accessed by third parties;

e. Whether Defendants' actions in failing to properly secure Plaintiff's and the Class members' Personal Sensitive Information proximately caused their injuries;

f. Whether Defendants failed to notify Plaintiffs and members of the Class in a timely manner that about the Data Breach;

g. Whether Plaintiff's and other Class members' Sensitive Information was compromised in the Data Breach and therefore injured;

h. Whether Plaintiff and other Class members are entitled to damages as a

result of Defendants' conduct.

i. Whether Plaintiff and other Class members are entitled to injunctive and declaratory relief.

80. Typicality: Plaintiff's claims are typical of the claims of the Class Members and have a common origin and basis. Plaintiff and Class Members are all persons injured the same uniform conduct, including the storage and sharing of Personal Sensitive Information by Defendants and their failure to safeguard it.

81. Adequacy: Plaintiff will fully and adequately assert and protect the interests of Class Members and has retained Class counsel who has considerable experience in class action litigation concerning corporate data security and has the resources necessary to prosecute this case vigorously on behalf of the Class. Neither Plaintiff nor her attorneys have any interests antagonistic to the interests of Class Members.

RULE 23(b)(3) FACTORS

82. The questions of law and fact common to all Class Members predominate over any questions affecting only individual Class Members.

83. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the Class Members' claims is economically infeasible and procedurally impracticable. Class Members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class Members to litigate their claims where it would otherwise be too expensive or inefficient to do so. Plaintiff knows of no difficulties in managing this action that would preclude

its maintenance as a class action.

84. Contact information for each Class Member, including mailing addresses, is readily available, facilitating notice of the pendency of this action.

85. **Injunctive and Declaratory Relief**. Class certification is also appropriate under Rule 23(b)(2). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, thus making injunctive and declaratory relief appropriate to the Class as a whole.

FIRST COUNT
Negligence
(On behalf of Plaintiff and the Nationwide Class)

86. Plaintiff realleges and incorporates by reference all preceding factual allegations.

87. Defendants required Plaintiff and the Class members to submit Personal Sensitive Information in order to obtain services and in consideration for Plaintiff and Class members paying for or using those services.

88. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants both had a duty of care to use reasonable means to secure and safeguard this Personal Sensitive Information to prevent disclosure of the information, and to guard the information from theft.

89. Defendants' duty included a responsibility to implement a process by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

90. Defendants also owed a duty of care to Plaintiff and members of the Class to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them adequately

protected their customers' Personal Sensitive Information.

91. Defendants' duty to use reasonable security measures arose as result of the special relationship that existed between LabCorp and/or Quest and their patients, which is recognized by laws including but not limited to HIPAA. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiff and the members of the Class from a data breach.

92. Defendants' duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendants are required to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

93. In addition, Defendants had a duty to use reasonable security measures 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.

94. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential Sensitive Information.

95. Defendants breached their common law, statutory and other duties—and thus, were negligent—by failing to use reasonable measures to protect patients' Personal Sensitive Information, and by failing to provide timely notice of the Data Breach.

96. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

i. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class members' Personal Sensitive Information;

ii. failing to adequately monitor the security of AMCA's network and systems;

iii. allowing unauthorized access to Plaintiff's and Class Members' Personal Sensitive Information;

iv. failing to recognize in a timely manner that Plaintiff's and other Class Members' Personal Sensitive Information had been compromised; and

v. failing to warn Plaintiff and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

97. It was foreseeable that Defendants' failure to use reasonable measures to protect Personal Sensitive Information and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

98. Plaintiff and the Class were not in a position to protect the Personal Sensitive Information that they provided to Defendants, but instead relied on Defendants to protect against the harms that Plaintiffs and the Class suffered as a result of the Data Breach.

99. Defendants have admitted that, as a result of the Data Breach, Plaintiff and the Class members' Personal Sensitive Information was compromised and disclosed to unauthorized third parties.

100. Defendants have breached their duty to Plaintiff and the Class by failing to exercise reasonable care to safeguard the Plaintiff and the Class members' Personal Sensitive Information while in Defendants' possession, by failing to implement adequate policies and systems to prevent

the Data Breach, and by failing to adequately disclose the existence and scope of the Data Breach to Plaintiff and the Class.

101. Defendants' failure to adequately implement measures to secure Personal Sensitive Information establishes a close temporal and causal connection to the harms suffered or risk of imminent harm suffered by Plaintiff and the Class.

102. As a consequence of Defendants' negligence, Plaintiff and the Class are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

SECOND COUNT
Negligence *Per Se*
(On behalf of Plaintiff and the Nationwide Class)

103. Plaintiff realleges and incorporates by reference all preceding factual allegations.

104. HIPAA was designed to protect the privacy of personal medical information by limiting its disclosure. Specifically, under HIPAA, Defendants are required to "reasonably protect" confidential patient data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. §164.530(c)(1). Additionally, under HIPAA, Defendants are obligated to provide notification of a breach of protected health information. 45 C.F.R. §§ 164.404 and 164.410. The confidential patient data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

105. HIPAA seeks to protect the privacy of protected confidential patient data by prohibiting any voluntary or involuntary use or disclosure of such data in violation of the directives set out in the statute and its regulations, and requiring notification in all instances when such data is breached.

106. Defendants are HIPAA-covered entities.

107. As described above, Defendants violated HIPAA by failing to maintain the confidentiality of their protected health information and to provide timely notification of the breach of such data.

108. Defendants' violation of HIPAA constitutes negligence *per se*.

109. Section 5 of the FTC Act prohibits "unfair. . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII, such as the credit card numbers and bank account information that were compromised in the Data Breach. The FTC publications and orders described above also form part of the basis of Defendants' duty.

110. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect credit card and bank account PII and by not complying with applicable industry standards, including PCI-DSS, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, length of time the information was maintained on an apparently vulnerable system, and foreseeable consequences of a data breach at a major, international medical services company, including, specifically, the immense damages that would result to patients.

111. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

112. Plaintiff and members of the Class are consumers and are within the class of persons that Section 5 of the FTC Act was intended to protect.

113. The harm that has occurred is the type of harm the FTC Act was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

114. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injury, including, but not limited to, the ongoing, imminent, and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; the loss of the confidentiality of the compromised patient data; and investing time and money in cancelling payment cards, changing or closing accounts, securing credit monitoring and identity theft insurance, and taking other steps to monitor their identities and protect themselves.

THIRD COUNT
Declaratory and Equitable Relief
(On behalf of Plaintiff and the Nationwide Class)

115. Plaintiff realleges and incorporates by reference all preceding factual allegations.

116. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and violate the terms of the federal and state statutes described herein.

117. Defendants still possess Personal Sensitive Information pertaining to Plaintiff and Class Members.

118. Defendants have not issued a statement that they have remedied the vulnerabilities in their practices and policies ensuring the data security of patients' Personal Sensitive Information.

119. Actual harm has arisen in the wake of the Data Breach regarding Defendants' duties of care to provide data security measures to Plaintiff and Class Members.

120. Defendants continue to owe a legal duty to safeguard Personal Sensitive Information of Plaintiff and the Class.

121. Defendants continue to breach this legal duty by failing to employ reasonable

measures to secure patient Personal Sensitive Information.

122. Plaintiff seeks a declaration that Defendants' existing data security measures do not comply with its obligations and duties of care and that Defendants must implement and maintain reasonable security measures, including, but not limited to:

i. Strengthen their data security systems and practices to ensure Personal Sensitive Information is adequately safeguarded;

ii. Engage in annual or other periodic audits of their data security systems and practices utilizing third-party security auditors and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on their systems on a periodic basis;

iii. Strengthen their practices to ensure "business associates" to whom Defendants provide Personal Sensitive Information engage in periodic audits of their data security systems and practices;

iv. Ensure that "business associates" to whom Defendants provide patients' Personal Sensitive Information audit, test, and train security personnel regarding use and storage of Personal Sensitive Information;

v. Ensure Personal Sensitive Information not necessary is deleted and destroyed and require that "business associates" used by Defendants delete and destroy such Personal Sensitive Information; and

vi. Provide free credit monitoring services to the Plaintiff and the Class.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members, respectfully request that this Honorable Court enter judgement as follows:

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

b. Awarding Plaintiff and Class Members appropriate relief, including actual and statutory damages;

c. Awarding equitable, injunctive, and declaratory relief as may be appropriate,

including without limitation an injunction and declaring Defendants' conduct to be unlawful;

d. Award Plaintiff and the Class reasonable attorneys' fees and costs of suit, as allowed by law and pursuant to O.C.G.A. 13-6-11; and,

e. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent allowable by law;

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

JURY DEMAND

Plaintiff, individually and on behalf of all those similarly situated, hereby requests a trial by jury.

Respectfully submitted this 23rd day of August, 2019.

THE FINLEY FIRM, P.C.

/s/ MaryBeth V. Gibson

MARYBETH V. GIBSON
State Bar No. 725843
mgibson@thefinleyfirm.com

Piedmont Center
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
T: (404) 320-9979

J. BENJAMIN FINLEY
State Bar No. 261504
bfinley@thefinleyfirm.com
Counsel for Plaintiff and the Proposed Class

200 13th Street
Columbus, GA 31901
T: (706) 322-6226