Exhibit C4

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

CHERYL CHUHA, individually and on behalf of a class of all others similarly situated, Plaintiff, v. QUEST DIAGNOSTICS INCORPORATED, LABORATORY CORPORATION OF AMERICA HOLDINGS, and OPTUM360, LLC, Defendants.	Case No. 19-742 **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Cheryl Chuha ("Plaintiff"), by and through her undersigned counsel, upon personal knowledge, as to herself and her own acts, and upon information and belief, as to all other matters, brings this putative class action against Defendants Quest Diagnostics Incorporated ("Quest"), Laboratory Corporation of America Holdings ("LabCorp"), and Optum360, LLC ("Optum360") (collectively, "Defendants") and alleges as follows:

INTRODUCTION

1. Plaintiff, individually and on behalf of all others similarly situated, brings this class action on behalf of all persons whose personal information was compromised as a direct result of Defendants' failure to safeguard millions of patients' highly sensitive protected health information, as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), medical information, and other personally identifiable information, including, but not limited to, names, Social Security numbers, credit card numbers, and bank account information (collectively referred to as "PII").

2. Quest and LabCorp are two of the largest clinical laboratory networks in the United

States. They provide clinical diagnostic services, such as blood testing, to the public, hospitals, clinics, and more. Plaintiff, like millions of other consumers, entrusted her sensitive personal, health, medical, and financial information to Defendants when she retained them for diagnostic services, relying on them care for and protect her PII.

3. Unfortunately, once Plaintiff and any of Quest or LabCorp's patients gave their PII to Quest and LabCorp, the PII was then shared with a variety of third-party vendors and subcontractors, such as Optum360 and AMCA, a billing collections service provider for both Quest and LabCorp.

4. Between August 1, 2018 and March 30, 2019, computer hackers breached AMCA's computer systems and gained unauthorized access to the millions of sensitive PII records of Quest and LabCorp's patients (the "Data Breach").

5. Quest announced on June 3, 2019 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' PII was compromised in the Data Breach.

6. The next day, 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

[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

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

7. Despite the fact that the threat of a data breach has been a well-known risk to Defendants, especially due to the highly valuable and sensitive nature of the data maintained by Defendants, Defendants failed to take reasonable steps to adequately protect the ultra-sensitive PII of its millions of patients. Plaintiff and the Class must now deal with the direct consequences of Defendants' failures.

8. The Data Breach was the inevitable result of Defendants' subpar security practices and lax approach to protecting PII. These data security deficiencies were so significant that computer hackers were able to access and maintain access to the PII undetected for over eight months.

9. Cyber criminals who steal sensitive PII are able to use this information to commit fraud and identify theft through opening bank accounts or loans in class members' names, obtaining medical services using class members' information, filing fraudulent tax returns with class members' information, obtaining government benefits or government-issued identification, and other forms of identity theft and fraud.

10. Despite the heightened risks Plaintiff and the class members now face because of the theft of their PII, Defendants waited nearly two months from the time the Data Breach was first discovered before disclosing that the Data Breach had occurred. Not only has this delay increased the risk of harm to Plaintiff and the Class members, Defendants have failed to fully inform the impacted patients of exactly what information was stolen nor the full extent of the Data Breach, depriving them of needed information they can use to take measures to protect themselves.

[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

11. As a direct result of Defendants' failure to adequately and reasonably protect their PII, Plaintiff and the Class members have incurred, and will continue to incur, significant damages in taking protective measures to reduce risk of identity theft and other fraudulent activity, and will now always be at an increased risk for identify theft, fraud, and other related harms.

12. Plaintiff seeks to recover damages and other relief resulting from the Data Breach, including but not limited to, compensatory damages, reimbursement of costs that she and others similarly situated have been forced to bear, and declaratory and injunctive relief to mitigate future harms that are certain to occur in light of the scope of the Data Breach.

PARTIES

13. Plaintiff Cheryl Chuha is a citizen of the Commonwealth of Pennsylvania. Ms. Chuha has been a regular patient of LabCorp and Quest for years. She last visited LabCorp for testing in June 2019 and Quest within the past two years. On information and belief, Ms. Chuha's PII was compromised in the Data Breach, and because of Defendants' failures to prevent the Data Breach, she will be at an increased risk for fraud, identity theft, and any related consequent damages.

14. Defendant Quest Diagnostics Incorporated is a corporation organized under the laws of Delaware, and is headquartered at 500 Plaza Drive, Secaucus, New Jersey 07094.

15. Defendant Laboratory Corporation of America Holdings is a corporation organized under the laws of Delaware, and is headquartered at 358 South Main Street, Burlington, North Carolina 27215.

16. Defendant Optum360, LLC is a limited liability company organized under the laws of Delaware, and is headquartered at 13625 Technology Drive, Eden Prairie, Minnesota 55344.

17. On information and belief, Defendant Optum360, LLC is contracted by Defendant

Quest Diagnostics Incorporated and Defendant Laboratory Corporation of America Holdings for billing collection services.

JURISDICTION AND VENUE

18. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 putative Class members (defined below); and minimal diversity exists because the majority of putative Class members, including the named Plaintiff, are citizens of a different state than Defendants.

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

20. Venue is proper in this District under 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 ALLEGATIONS

A. Background

21. Quest is "the world's leading provider of diagnostic information services", has thousands of patient centers located around the United States, and purportedly "annually serves one in three adult Americans and half the physicians and hospitals in the United States".[3]

22. LabCorp is also a major, global clinical laboratory service that "provides diagnostic, drug development and technology-enabled solutions for more than 120 million patient

[3] "Fact Sheet", Quest Diagnostics Incorporated, *available at* http://newsroom.questdiagnostics.com/index.php?s=30664 (last accessed June 21, 2019).

encounters per year [and] typically processes tests on more than 2.5 million patient specimens per week".[4]

23. As part of its operations, Quest relies on Optum360 and its sub-vendor, AMCA, for billing collections services.

24. LabCorp also relies on AMCA for its billing collection services.

25. When patients retain Quest or LabCorp for diagnostic and laboratory services, Quest and LabCorp collect, store, and maintain extensive amounts of highly sensitive protected health information and other personally identifiable information about those patients, which is then routinely shared with their respective vendors and subcontractors.

B. Plaintiff and the Class Relied on Defendants to Adequately Protect Their Sensitive Information

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

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

C. The Data Breach

a. Quest

28. On June 3, 2019, Quest announced a data security incident involving its billing collections vendor, AMCA.

[4] Form 10-K at 4, Laboratory Corporation of America Holdings, filed February 28, 2019, *available at* https://www.sec.gov/Archives/edgar/data/920148/000092014819000033/lh10-k2018.htm

29. According to a Form 8-K that Quest filed with the Securities and Exchange Commission:

> On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest Diagnostics Incorporated ("Quest Diagnostics") and Optum360 LLC, Quest Diagnostics' revenue cycle management provider, of potential unauthorized activity on AMCA's web payment page. Quest Diagnostics and Optum360 promptly sought information from AMCA about the incident, including what, if any, information was subject to unauthorized access.
>
> Although Quest Diagnostics and Optum360 have not yet received detailed or complete information from AMCA about the incident, AMCA has informed Quest Diagnostics and Optum360 that:
>
> - 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 information on AMCA's affected system included financial information (e.g., credit card numbers and bank account information), medical information and other personal information (e.g., Social Security Numbers);
> - as of May 31, 2019, AMCA believes that the number of Quest Diagnostics patients whose information was contained on AMCA's affected system was approximately 11.9 million people….[5]

30. Although Quest and Optum360 claimed they first became aware of the breach to AMCA's system on May 14, 2019, the breach was apparently discovered much earlier, as early as March 2019. It wasn't until June 2019 that Quest publicly disclosed the existence of the Data Breach to the public.

[5] Form 8-K, Quest Diagnostics Incorporated, filed June 3, 3019, *available at* https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm

b. LabCorp

31. 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.[6]

32. LabCorp did not disclose or indicate at what point it first learned of the Data Breach or whether it was aware of the Data Breach prior to June 4, 2019.

D. The Data Breach Was the Result of Defendants' Data Security Failures and Was a Foreseeable Risk

33. The Data Breach was the direct result of Defendants' actions and choices, which resulted in inadequate data security practices and the breach of systems containing PII.

34. The harm to Plaintiff resulting from Defendants' inadequate and insufficient data security systems and practices was at all times entirely foreseeable to Defendants.

[6] *Supra* n. 2.

35. Quest was aware of its obligations and duties to protect its patients' PII, as evidenced by the Notice of Privacy Practices that Quest maintains on its website:

> Quest Diagnostics and its wholly owned subsidiaries (collectively "Quest Diagnostics") are committed to protecting the privacy of your identifiable health information. This information is known as "protected health information" or "PHI." PHI includes laboratory test orders and test results as well as invoices for the healthcare services we provide.
>
> Our Responsibilities
>
> Quest Diagnostics is required by law to maintain the privacy of your PHI. We are also required to provide you with this Notice of our legal duties and privacy practices upon request. It describes our legal duties, privacy practices and your patient rights as determined by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. We are required to follow the terms of this Notice currently in effect. We are required to notify affected individuals in the event of a breach involving unsecured protected health information. PHI is stored electronically and is subject to electronic disclosure. This Notice does not apply to non-diagnostic services that we perform such as certain drugs of abuse testing services and clinical trials testing services.[7]

36. As reflected on Quest's most recent Form 10-K filing, the costs and risks associated with substandard information technology practices were known to and understood by Quest:

> **Hardware and software failures or delays in our information technology systems, including failures resulting from our systems conversions or otherwise, could disrupt our operations and cause the loss of confidential information, customers and business opportunities or otherwise adversely impact our business.**
>
> IT systems are used extensively in virtually all aspects of our business, including clinical testing, test reporting, billing, customer service, logistics and management of medical data. Our success depends, in part, on the continued and uninterrupted performance of our IT systems. A failure or delay in our IT systems could impede

[7] Notice of Privacy Practices, Quest Diagnostics Incorporated, *available at* http://www.questdiagnostics.com/hom/privacy-policy/notice-privacy-practices.html (last accessed June 21, 2019).

> our ability to serve our customers and patients and protect their confidential personal data. Despite redundancy and backup measures and precautions that we have implemented, our IT systems may be vulnerable to damage, disruptions and shutdown from a variety of sources, including telecommunications or network failures, system conversion or standardization initiatives, human acts and natural disasters. These issues can also arise as a result from failures by third parties with whom we do business and for which we have limited control. Any disruption or failure of our IT systems could have a material impact on our ability to serve our customers and patients, including negatively affecting our reputation in the marketplace.[8]

37. Quest was also acutely aware that its systems are "subject to potential cyber-attacks or other security breaches" that could result in "unauthorized persons misappropriating… confidential data, including patient data that we obtain, transmit and store on and through our IT systems." *Id.*

38. And Quest was aware that the same cyber security risks apply to its vendors and sub-contractors:

> Third parties to whom we outsource certain of our services or functions, or with whom we interface, may store our confidential, patient data or other confidential information, are also subject to the risks outlined above. A breach or attack affecting these third parties could also harm our business, results of operations and reputation.

Id. at 36.

39. Perhaps most telling of all, however, is the fact that Quest previously suffered a data breach several years ago: "In December 2016, we reported that an internet application on our IT network had been the target of an external cyber-attack, resulting in the theft of certain patient data." *Id.* at 35. And Quest has regularly "experienced other attacks, viruses, attempted intrusions

[8] Form 10-K at 35, Quest Diagnostics Incorporated, filed February 21, 2019, *available at* https://www.sec.gov/Archives/edgar/data/1022079/000102207919000030/dgx1231201810-k.htm

or similar problems", of which Quest understood the incumbent consequences of failing to vigilantly protect against. *Id.*

40. LabCorp was aware of its obligations and duties to protect its patients' PII, 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]

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

> 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]

[9] LabCorp, "HIPAA Notice of Privacy Practices", *available at* https://www.labcorp.com/hipaa-privacy/hipaa-information (last accessed June 21, 2019).

[10] Form 10-K at 33, *supra* n. 4.

42. 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 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]

43. 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 PII 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

[11] *Id.*

> 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 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]

44. Indeed, LabCorp 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]

45. Moreover, Defendants were aware that the medical industry is a prime target for cyber criminals, and that the medical industry has already experienced a substantial number of

[12] *Id.* at 41 (emphasis added).

[13] *Id.* at 48-49.

data breaches targeting patient-related data, including several high profile breaches occurring at Anthem Inc., Premera Blue Cross, Excellus Health Plan Inc., and the University of California, Los Angeles Health, among others, which each resulted in the loss of millions of individuals' sensitive information.[14]

46. Thus, Defendants knew, given the vast amount of PII they managed and maintained, and through personal experience, that they were a target of attempted cyber and other security threats, and therefore 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.

E. Defendants Violated Federal Security Requirements and Other Industry Standards

47. Defendants have an unambiguous duty to maintain the confidentiality of patients' PII and to prevent any third-party misuse or access to such information. Defendants' actions and failure to safeguard patients' information violated federal law, federal data security standards, and industry standards, as well as an established legal duty to not act negligently when handling and storing PII.

F. Defendants Failed to Comply with HIPAA

48. The lax data security practices and systems employed by Defendants which resulted in the Data Breach indicate that Defendants 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 PII should be safeguarded. Defendants have failed to comply with those safeguards by, *inter alia*:

---

[14] *See* HIPAA Journal, "Healthcare Data Breach Statistics", *available at* https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last accessed June 21, 2019).

a. Failing to adequately protect patients' PII;

b. Failing to properly monitor data security systems for existing intrusions;

c. Failing to ensure vendors and other third-parties entrusted with PII were employing reasonable data security practices;

d. Failing to maintain adequate data security systems to prevent intrusions and other forms of cyber-attacks or data loss;

e. Failing to ensure the confidentiality and integrity of electronic protected health information that was created, received, maintained and/or transmitted, pursuant to 45 C.F.R § 164.306(a)(1);

f. Failing to implement policies and procedures for electronic systems where electronic protected health information was stored to allow access only to persons or software programs that have been granted access, pursuant to 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, pursuant to 45 C.F.R. § 164.308(a)(1);

h. Failing to ensure compliance with security rules for workforces, pursuant to 45 C.F.R. § 164.306(a)(94);

i. Failing to protect against reasonably anticipated disclosures or uses of electronic protected health information that are not permitted under privacy rules, pursuant to 45 C.F.R. § 164.306(a)(3);

j. Failing to protect against reasonably anticipated hazards or threats to the security or integrity of electronic protected health information, pursuant to 45 C.F.R. § 164.306(a)(2);

k. Failing to identify and respond to suspected or known security incidents, including a failure to mitigate harmful effects of security incidents that are known, pursuant 45 C.F.R. § 164.308(a)(6)(ii);

l. Failing to adequately train all workforce members, including third-party contractors, on protected health information policies and procedures as necessary and appropriate for the workforce to carry out their functions and maintain security, pursuant to 45 C.F.R. §§ 164.530(b) and 308(a)(5); and,

m. Failing to adequately 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 Federal Trade Commission Requirements

49. 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.

50. 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.

51. 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.

52. 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.

53. 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 Industry Standards for Data Security

54. 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.

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

56. 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.

57. PCI DSS v.3.2, the version of the standard in effect beginning in April 2016, imposes the following 12 "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

Furthermore, PCI DSS v.3.2 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates.

58. Among other things, 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. As discussed herein, Defendants failed to comply with these requirements.

I. Plaintiff and the Class Have Been, Are Currently Being, and Will Be Harmed by the Data Breach

59. The Data Breach has inflicted immediate, hard costs on Plaintiff and members of the Class.

60. Defendants failed to follow HIPAA-mandated safeguards and industry standards, and failed to effectively monitor their security systems to ensure the safety of patient information.

Defendants' substandard security protocols and failure to adequately monitor for unauthorized intrusion, as well as a failure to monitor third-parties with access to or who possess patients' PII, caused Plaintiff and the Class members' PII to be compromised for a significant period of time without detection by Defendants.

61. Plaintiff and the Class have incurred, and will continue to incur, substantial damage because of Defendants' failures to meet reasonable standards of data security.

62. As a result of the Defendants' Data Breach, Plaintiff and the Class are required to incur costs for protective measures such as credit monitoring, cancelling payment cards, changing or closing accounts, investigating fraudulent activity, and taking other steps to protect themselves in an effort to reduce the risk of future, but certainly impending, identity theft, loan fraud, and other fraudulent transactions.

63. Sensitive personal and financial information, like the information compromised in this breach, is extremely valuable. Criminals have gained access to highly sought-for PII. They can now use this data to steal the identities of the patients whose information has been compromised or sell it to others who plan to do so. In this manner, unauthorized third-parties can assume the stolen identities (or create entirely new identities from scratch) to obtain medical services, make transactions or purchases, open credit or bank accounts, apply for loans, forge checks, commit immigration fraud, obtain a driver's license in the patient's name, obtain government benefits, or file a fraudulent tax return. A report by the Department of Justice found that 86% of identity theft victims in 2014 experienced the fraudulent use of existing account information, including credit card and bank account information.[15]

[15] Erika Harrell, Ph.D., "Victims of Identity Theft", 2014, U.S. DEP'T OF JUST., BUREAU OF JUST. STAT. (Sept. 2015), *available at* https://www.bjs.gov/content/pub/pdf/vit14.pdf.

64. Consumers inevitably face significant emotional distress after theft of their identity. The fear of financial harm can cause significant stress and anxiety for many consumers. According to the DOJ, an estimated 36% of identity theft victims experienced moderate or severe emotional distress as a result of the crime. *Id.*

CLASS ALLEGATIONS

65. Plaintiff brings this action on behalf of herself and as a class action under Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of the following nationwide class, defined as follows:

> All individuals legally residing in the United States who used Quest and/or LabCorp's services, provided PII to Quest and/or LabCorp, and whose PII was compromised as a result of the Data Beach.

The Rule 23(a) Factors

66. This action may properly be maintained as a class action and satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

67. Numerosity: The members of the Class are so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective class members through this class action will benefit both the parties and the Court, and will facilitate judicial economy.

68. Typicality: Plaintiff's claims are typical of the claims of the absent members of the Class and have a common origin and basis. Plaintiff and Class members are all persons injured by Defendants' Data Breach. Plaintiff's claims arise from the same practices and course of conduct giving rise to the claims of the absent Class members and are based on the same legal theories, namely, the Defendants' Data Breach. If prosecuted individually, the claims of each Class member

would necessarily rely upon the same material facts and legal theories and would seek the same relief.

69. Common Questions of Fact and Law: There are common questions of law and fact that predominate over questions affecting only individual Class members. These common legal and factual questions include, but are not limited to:

a. whether Defendants owed a duty to Plaintiff and the members of the Class to protect PII;

b. whether Defendants failed to provide reasonable security to protect PII;

c. whether Defendants negligently or otherwise improperly allowed PII to be accessed by third parties;

d. whether Defendants failed to adequately notify Plaintiff and members of the Class that their data systems were breached;

e. whether Plaintiff and the members of the Class were injured and suffered damages and ascertainable losses;

f. whether Defendants' actions, which failed to reasonably secure Plaintiff and the Class member's PII, proximately caused the injuries suffered by Plaintiff and the members of the Class;

g. whether Plaintiff and members of the Class are entitled to damages and, if so, the measure of such damages; and,

h. whether Plaintiff and the members of the Class are entitled to declaratory and injunctive relief.

70. Adequacy of Representation: Plaintiff will fully and adequately assert and protect the interests of the absent Class members and has retained Class counsel who have considerable

experience in class action litigation concerning corporate data security and possess the resources necessary to prosecute this case. Neither Plaintiff nor her attorneys have any interests contrary to or conflicting with the interests of the absent Class members.

The Rule 23(b)(2) and (b)(3) Factors

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

72. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent 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.

73. Contact information for each Class member, on information and belief, is readily available, facilitating notice of the pendency of this action.

74. Defendants have acted on grounds that apply generally to the Class as a whole, making injunctive relief appropriate on a class wide basis, pursuant to Fed. R. Civ. P. 23(b)(2).

CAUSES OF ACTION

COUNT I
Negligence

75. Plaintiff incorporates by reference each and every allegation contained in the previous paragraphs.

76. In order to retain LabCorp or Quest's services, LabCorp and Quest required Plaintiff and the Class to provide their PII. LabCorp and Quest then forwarded this information to Optum360 and/or AMCA.

77. Plaintiff and the Class provided their PII to LabCorp and Quest with the understanding that the PII would be treated with reasonable measures to secure and safeguard it, including by any third-party vendors and sub-contractors.

78. Defendants undertook a duty to exercise reasonable care in protecting and securing Plaintiff and the Class members' PII from inadvertent disclosure, misuse, and from being compromised, lost, or stolen.

79. Defendants' duty also included a responsibility to design, maintain, and ensure security practices and systems are implemented in a manner to adequately safeguard PII, consistent with HIPAA, the FTC Act, and industry standards.

80. Defendants were also responsible for ensuring that employees who were tasked with maintaining PII were adequately trained to handle PII, including training on cyber security and the protection of PII.

81. Defendants were fully aware of the sensitive nature of the PII entrusted to them and the risks as well as potential harms that Plaintiff and the Class would suffer if their PII were compromised.

82. Defendants knew or should have known of the risks associated with the collection and storage of PII, as well as the magnitude of providing adequate safeguards for PII, especially in the current climate of rampant cyber-crimes and hacking occurring in the medical industry.

83. Defendants' conduct created a foreseeable risk of harm to Plaintiff and the Class by failing to take measures to prevent the Data Breach and failing to comply with HIPAA, the FTC Act, and industry standards for the safeguarding of PII.

84. Defendants' duty to use reasonable security measures to prevent the Data Breach arose as a result of the special relationship that existed between Defendants and the Plaintiff and the members of the Class. The special relationship arose because Plaintiff and the members of the Class entrusted Defendants with their confidential patient data, as part of the diagnostic services process. 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.

85. Defendants' duty to use reasonable security measures arose under HIPAA, pursuant to which 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). The confidential patient data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

86. Defendants' duty to use reasonable security measures arose under Section 5 of the FTC 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 patient data by healthcare providers like Defendants. The FTC publications and data security breach orders described above further form the basis of Defendants' duty.

87. Defendants' duty to use reasonable care in protecting PII arose not only as a result of the common law and the statutes and regulations described above, but also because they had committed to comply with industry standards for the protection of confidential patient data.

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

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

90. Defendants have breached their duty to Plaintiff and the Class by failing to exercise reasonable care to safeguard the Plaintiff and the Class members' PII 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.

91. But for Defendants' negligence in breaching their duties owed to Plaintiff and the Class, Plaintiff and the Class members' would not have had their PII compromised.

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

93. 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.

COUNT II
Negligence *Per Se*

94. Plaintiff incorporates by reference each and every allegation contained in the previous paragraphs.

95. 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.

96. 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.

97. Defendants are HIPAA-covered entities.

98. 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.

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

100. 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.

101. 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.

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

103. 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.

104. 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.

105. 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.

COUNT III
Declaratory and Equitable Relief

106. Plaintiff incorporates by reference each and every allegation contained in the previous paragraphs.

107. 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.

108. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure patient PII;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure patient PII; and,

c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiff and the Class harm.

109. The Court also should issue corresponding injunctive relief requiring Defendants to employ adequate security protocols, consistent with industry standards, to protect PII. Specifically, this injunction should, among other things, direct Defendants to:

a. Take measures to strengthen their data security systems and practices to ensure PII is adequately safeguarded;

b. Undertake annual or other periodic audits of their data security systems and practices; and,

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court:

A. Certify the Class appoint Plaintiff and Plaintiff's counsel to represent the Class;

B. Enter a monetary judgment in favor of Plaintiff and the Class to compensate them for the injuries they have suffered, together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

A. Enter a declaratory judgment as described herein;

B. Grant the injunctive relief requested herein;

C. Award Plaintiff and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and,

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims so triable.

Dated: June 21, 2019

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch
CARLSON LYNCH, LLP
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
glynch@carlsonlynch.com

Katrina Carroll
CARLSON LYNCH, LLP
111 W. Washington Street
Suite 1240
Chicago, IL 60602
Tel: (312) 750-1265
kcarroll@carlsonlynch.com

Joseph P. Guglielmo
SCOTT+SCOTT
Attorneys at Law LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Tel: (212) 223-6444
jguglielmo@scott-scott.com

Jonathan M. Jagher
Kimberly A. Justice
FREED KANNER LONDON
& MILLEN, LLC
923 Fayette Street
Conshohocken, PA 19428
Tel: (610) 234-6487
jjagher@fklmlaw.com
kjustice@fklmlaw.com

Attorneys for Plaintiff