Exhibit C16

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

PETER D. SMITH, AND EMILY SMITH, individually and on behalf of all others similarly situated, Plaintiffs, v. OPTUM 360 LLC, QUEST DIAGNOSTICS INCORPORATED, AND LABORATORY CORPORATION OF AMERICA HOLDINGS, Defendants.	Case No. **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

Plaintiffs Peter D. Smith and Emily Smith, individually and on behalf of the proposed Class defined below, allege as follows upon personal knowledge, experience, information and belief, including investigation conducted by their attorneys.

I. NATURE OF THE CASE

1. Plaintiffs bring this class action law suit against Defendants Quest Diagnostics Incorporated ("Quest"), Optum360 LLC ("Optum360") and Laboratory Corporation of America Holdings ("LabCorp") (collectively, "Defendants"), because of their failure to protect the confidential information of millions of consumers – including their names, credit card numbers, bank account information, Social Security numbers, "medical information," and other protected health information as defined by the Health

Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Sensitive Information").[1]

2. Quest is the world's leading provider of diagnostic testing, information and services.[2] Quest annually serves one in three adult Americans and half the physicians and hospitals in the United States.[3]

3. Optum360 contracts with Quest to provide revenue cycle management services. In turn, Optum360 contracted with American Medical Collection Agency ("AMCA") for customer billing services.[4]

4. LabCorp is a leading "global life sciences company that is deeply integrated in guiding patient care through its comprehensive clinical laboratory and end-to-end drug development services."[5] LabCorp provides "diagnostic, drug development and technology-enabled solutions for more than 120 million patient encounters per year."[6]

5. In order to receive diagnostic services from Quest or LabCorp ("Diagnostic Services Defendants"), an individual must give them his or her Sensitive Information. Plaintiffs and the proposed Class members took reasonable steps to preserve the confidentiality of their Sensitive Information in many ways, including protecting the Sensitive Information with confidential passwords and relying on physician-patient privilege and confidentiality.

---

[1] https://www.law360.com/articles/1165388/quest-diagnostics-says-breach-hit-11-9-million-patients
[2] https://www.questdiagnostics.com/home/about/vision.html
[3] https://www.questdiagnostics.com/home/about/products-services.html
[4] https://www.law360.com/articles/1165388/quest-diagnostics-says-breach-hit-11-9-million-patients; https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm (Quest 8-K filed with the Securities and Exchange Commission 6/3/2019.)
[5] https://www.labcorp.com/about-us
[6] *Id.*

6. Quest provides individuals' Sensitive Information to Optum360 and AMCA for use in AMCA's billing and collection services on Quest's behalf.

7. LabCorp provides individuals' Sensitive Information to AMCA for use in AMCA's billing and collection services on LabCorp's behalf.

8. As providers of health care services, the Diagnostic Services Defendants and their agents including Defendant Optum360 and AMCA are required to protect their patients' Sensitive Information, including by adopting and implementing specific data security regulations and standards set forth under HIPAA.

9. In addition to their implied statutory obligations, the Diagnostic Services Defendants expressly promise – through their Notices of Privacy Practices, public statements, and other written assurances – to safeguard and protect Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards.

10. Unfortunately, Defendants' failure to protect the Sensitive Information in their control resulted in a massive data breach. On June 3, 2019, Quest revealed that AMCA had notified them that its web payment page had been hacked and the Sensitive Information of approximately 11.9 million Quest patients was compromised (the "Data Breach").[7] On June 5, 2019, LabCorp revealed that AMCA had recently told them the Sensitive Information of approximately 7.7 million LabCorp patients had been compromised in the same Data Breach.[8]

[7] *Id.*
[8] https://healthitsecurity.com/news/7.7m-labcorp-patients-included-in-amca-breach-victims-with-quest

11. According to Quest, AMCA had notified Quest and Optum360 on May 14, 2019 of the Data Breach, and the unauthorized user had access to the Sensitive Information between August 1, 2018 and March 30, 2019.[9]

12. LabCorp has not indicated the date AMCA first told them of the Data Breach, but it does indicate that AMCA told them the unauthorized user had access to the Sensitive Information during the same dates: August 1, 2018 to March 30, 2019.[10]

13. The Data Breach not only revealed that Defendants failed to provide the level of data protection that they promised and that their patients paid for, it also exposed millions of individuals' Sensitive Information to an increased risk of misuse by unauthorized third parties (i.e. identity theft). In fact, affected individuals face a particularly real risk of misuse here (to the extent their information has not been misused already) because their Sensitive Information was specifically targeted by hackers seeking to steal consumer data.

14. Had Defendants informed Plaintiffs and other members of the proposed Class that they would use inadequate security measures – including by using data security practices at odds with their own affirmative representations – individuals would not have been willing to use or pay for Diagnostic Services Defendants' services at the prices charged, if at all, and would not have been willing to provide their Sensitive Information to Defendants.

[9] *Id.*
[10] https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm

15. Defendants' failure to implement adequate security protocols jeopardized millions of patients' Sensitive Information, fell well short of their statutory and professional standard obligations, fell short of Plaintiffs' and other proposed Class members' reasonable expectations when they provided their Sensitive Information to Defendants, and diminished the value of the services that Defendants provided. In other words, because Defendants failed to disclose their gross security inadequacies, they delivered a fundamentally less useful and less valuable service than the ones for which patients paid.

Accordingly, Plaintiffs bring suit, on behalf of themselves and all others similarly situated, to seek redress for Defendants' unlawful conduct.

II. PARTIES

16. Plaintiff Peter D. Smith is a natural person and a citizen of the State of Minnesota. Plaintiff Peter D. Smith brings this action on behalf of himself and the Nationwide Class, as defined below. Plaintiff has been a patient of Quest whose Sensitive Information, on information and belief, was compromised in the Data Breach.

17. Plaintiff Emily Smith is a natural person and a citizen of the State of Minnesota. Plaintiff Emily Smith brings this action on behalf of herself and the Nationwide Class, as defined below. Plaintiff has been a patient of Quest whose Sensitive Information, on information and belief, was compromised in the Data Breach.

18. Defendant Quest Diagnostics Incorporated is a provider of diagnostic tests and services and a corporation existing under the laws of the State of Delaware with its

headquarters located at 500 Plaza Drive, Secaucus, New Jersey 07094. It has patient locations in 44 states (including Minnesota), Washington, D.C. and Puerto Rico.

19. Defendant Optum360 LLC is a provider of information technology and services to the health care industry and a corporation existing under the laws of the State of Delaware with its headquarters located at 11000 Optum Circle, Eden Prairie, Minnesota 55344. It does business throughout the country, including in the State of Minnesota.

20. Defendant Laboratory Corporation of America Holdings is a provider of diagnostic tests and services and a corporation existing under the laws of the State of Delaware with its headquarters located at 358 South Main Street, Burlington, North Carolina 27215. It does business throughout the country, including the State of Minnesota.

III. JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2) and (d)(5) because (a) at least one member of the putative Class is a citizen of a state different from at least one Defendant, (b) the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (c) there are more than 100 putative Class members.

22. This Court has personal jurisdiction over Defendants because they are registered to and regularly do conduct business in this District, and a portion of the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated, in part, from this District.

23. Venue is proper pursuant to 28 U.S.C. § 1391(b)(1) because Defendant Optum360 is headquartered in this District and all Defendants are residents for venue

purposes because they regularly transact business here. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated from this District. Venue is additionally proper because Defendants are registered to and do conduct business in this District.

IV. FACTUAL BACKGROUND

A. Diagnostic Services Defendants Collect Sensitive Information from Patients and Store It on Their Computer Systems.

24. Diagnostic Services Defendants Quest and LabCorp each operate thousands of "Patient Service Centers" around the country where they draw and process patients' blood and/or other specimens for various diagnostic tests following an order from a doctor.

25. In order to access Diagnostic Services Defendants' services, patients must provide them with a variety of Sensitive Information, including photo identification, health insurance information and payment method information (regardless whether the patient has health insurance). In addition, Diagnostic Services Defendants receive Sensitive Information, including confidential medical information, from the patient's doctor.

26. Patients are billed for Diagnostic Services Defendants' services separately from their physicians' bills, either by going to a Service Center themselves, or if their doctor sends their specimen to one of their diagnostic laboratories for testing.

27. Defendant Quest contracts with Defendant Optum360 as its revenue cycle management provider. Defendant Optum360 in turn brought in AMCA as a billing collections vendor. Defendant Quest provided Plaintiffs' and the proposed Class members'

Sensitive Information to Defendant Optum360 and to AMCA, in connection with their contracts for services.

28. Defendant LabCorp contracts with AMCA as a billing collections vendor. Defendant LabCorp provided Plaintiffs' and the proposed Class members' Sensitive Information to AMCA in connection with their contracts for services.

B. Defendants Had a Duty and Contractual Obligation to Protect Their Patients' Sensitive Information from Unauthorized Disclosures.

29. Defendants had a duty and obligation to keep the Sensitive Information they obtained confidential and to protect that information from unauthorized disclosures. Diagnostic Services Defendants' websites and their contracts with their patients commit them to protecting their Sensitive Information. As vendors/contractors for Diagnostic Services Defendant(s), Defendant Optum360 and AMCA are obligated to maintain Diagnostic Services Defendants' obligations and promises to their patients to keep their Sensitive Information confidential.

30. Defendants have obligations to maintain the safety and confidentiality of their patients' Sensitive Information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), their contractual commitments, and state law.

31. Defendant Quest's website has the question "Is my payment information secure?" on its "Frequently Asked Questions" page. Quest responds "Yes" and explains that it uses "Transport Security Layer (TSL) to encrypt your credit card number, name, and address information *so only QuestDiagnostics.com is able to decode your information*."[11]

[11] https://myquest.questdiagnostics.com/myquest-faq1/QuestDirect.htm (Emphasis added.) (Last visited 6/14/2019).

32. Defendant Quest's privacy policy as published on its website extends its promise of confidentiality to include the obligation of Defendant Optum360 and of AMCA: "[O]ur contractors to who we may provide such information for the limited purpose of providing services to us . . . are obligated to keep the information confidential."[12] Defendant Quest further commits that "we limit Quest Diagnostics' employees and contractors' access to personal information. Only those employees and contractors with a business reason to know have access to this information."[13]

33. Defendant Quest posts the same Notice of Privacy Practices on its website, acknowledging its duty and that of its contractors and vendors to protect all Sensitive Information in their possession.[14] For example, Defendant Quest's "Notice of Privacy Policies" states that Quest is "required to notify affected individuals in the event of a breach involving unsecured protected health information, and that any outside collection agencies it may use are "required to maintain the privacy and security of" personal health information ("PHI" -- one important category of the Sensitive Information that Defendant have compromised in this case.)[15]

34. Defendant LabCorp publishes its Web Privacy Policy on its website. In response to its own question: "How does LabCorp protect the security of your information?," LabCorp responds:

> "Financial information and payment data, including credit card numbers, that you provide to us via the LabCorp internet bill payment link is encrypted by using secure socket layer (SSL) encryption technology, which employs a

[12] https://www.questdiagnostics.com/home/privacy-policy/online-privacy.html (Last visited 6/14/2019).
[13] *Id.*
[14] https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html (Last visited 6/14/2019).
[15] *Id.*

> 128-bit encryption system. This information *may be accessed only by LabCorp employees who maintain password and job-required access rights, and third party vendors who support LabCorp's billing operations.* Additionally, LabCorp maintains all personal patient data within the LabCorp information system (IS) firewalls that operate on separate LabCorp mainframes/servers. *The general public may not access these mainframes/servers.* [16]

35. Defendant LabCorp also publishes its "HIPAA Information—LabCorp's Notice of Privacy Practices" on its website, where it acknowledges its duty and that of its contractors and vendors to protect all Sensitive Information in their possession: "LabCorp is required to provide patient notification if it discovers a breach of unsecured PHI unless there is a demonstration, based on a risk assessment, that there is a low probability that the PHI has been compromised. *You will be notified without unreasonable delay* and no later than 60 days after discovery of the breach." [17] LabCorp further states: "All of our business associates are required to maintain the privacy and confidentiality of your PHI." [18]

C. Defendants Failed To Protect Patients' Sensitive Information Properly.

36. On June 3, 2019, Defendant Quest filed a Form 8-K with the Securities and Exchange Commission, in which it disclosed for the first time that: "On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest Diagnostics Incorporated ("Quest Diagnostics") and Optum360 LLC, Quest

[16] https://www.labcorp.com/hipaa-privacy/web-privacy-policy (Emphasis added.) (Last visited 6/14/2019).
[17] https://www.labcorp.com/hipaa-privacy/hipaa-information (Emphasis added.) (Last visited 6/14/2019).
[18] *Id.*

Diagnostics' revenue cycle management provider, of potential unauthorized activity on AMCA's web payment page."[19]

37. According to Defendant Quest's Form 8-K, AMCA informed Defendants Quest and Optum360 that "between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that . . . included financial information (e.g. credit card numbers and bank account information), medical information and other personal information (e.g. Social Security Numbers). . ." of approximately 11.9 million Quest Diagnostics patients.[20]

38. On June 5, 2019, Defendant LabCorp filed a Form 8-K with the Securities and Exchange Commission, in which it disclosed for the first time that approximately 7.7 million of its patients' Sensitive Information had been compromised in the same AMCA Data Breach and during the same dates ("between August 1, 2018 and March 30, 2019").[21]

39. On February 28, 2019, Gemini Advisory, a data security analysis firm "identified a large number of compromised payment cards while monitoring dark web marketplaces. Almost 15% of these records included additional personally identifiable information (PII), such as dates of birth (DOBs), Social Security numbers (SSNs) and physical addresses."[22] On March 1, 2019, Gemini attempted to notify AMCA but got no

[19] https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm (Last visited 6/14/2019).
[20] *Id.*
[21] http://secfilings.nasdaq.com/filingFrameset.asp?FilingID=13474097&RcvdDate=6/4/2019&CoName=LABORATORY%20CORP%20OF%20AMERICA%20HOLDINGS&FormType=8-K&View=html
[22] https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/

response. Gemini then contacted federal law enforcement, who reportedly followed up with AMCA.[23]

40. After being contacted by federal law enforcement, AMCA disabled its payment portal, at least as early as April 8, 2019.[24] By AMCA's own report, the hacker's unauthorized access ended on March 30, 2019,[25] which suggests that they may have disabled its payment portal by then.

D. Defendants Violated HIPAA, Industry Standard Data Protection Protocols and Their Own Representations Regarding Data Security.

41. HIPAA requires that healthcare providers like Quest and LabCorp and their contractors and vendors like Optum360 and AMCA adopt administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of patients' Sensitive Information.

42. Unfortunately, Defendants' Data Breach resulted from a variety of failures to follow HIPAA-mandated data security protocols, many of which are also industry standard.

43. More specifically, Defendants' Data Breach demonstrates that they failed to honor their duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

[23] *Id.*
[24] *Id.*
[25] https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm

b. Adequately protecting Plaintiffs' and the proposed Class members' Sensitive Information;

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

d. Implementing 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);

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

f. Implementing 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);

g. Protecting 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);

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

i. Ensuring compliance with the HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(4); and

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

44. Likewise, Defendants' security lapses demonstrate that they failed to follow through on their own representations about their data security practices, including those discussed above. Specifically, Defendants did not:

a. Take precautions to protect users' Sensitive Information, whether online or offline;

b. Maintain the confidentiality or privacy of the Sensitive Information – as defined by their Notices of Privacy Practices – in their control, specifically including information stored in electronic form;

c. Take steps to secure their electronic systems from unauthorized access;

d. Train their employees on their confidentiality policies and procedures;

e. Enforce their confidentiality policies and procedures;

f. Timely or reasonably notify affected individuals following the Data Breach;

g. Protect individuals' privacy by making sure their information stayed confidential, including by failing to enforce or monitor employee compliance with their confidentiality policies and practices;

h. Ensure the security of their facilities and electronic systems to prevent unauthorized access to their patients' Sensitive Information; and

i. Remain aware of or follow corporate policies, processes and procedures designed to secure electronic systems in compliance with HIPAA Security requirements.

45. Had Defendants implemented the above-described data security protocols or policies, the consequences of the Data Breach could have been avoided, or at least significantly reduced (as the breach could have been detected more than six months earlier, the amount of Sensitive Information compromised could have been greatly reduced or avoided entirely, and affected patients could have been notified – and taken protective/mitigating actions – much sooner).

46. Even though Defendants promised their patients the above-described security measures, they were not adequately implemented (if at all), which resulted in the unauthorized release of Sensitive Information.

E. It is Well-Established That Security Breaches Lead to Instances of Identity Theft.

47. 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 SSNs to open financial accounts, receive government benefits and incur charges and credit in a person's name.[26] As the GAO Report states, this type of identity theft is the most

[26] *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* http://www.gao.gov/new.items/d07737.pdf (Last visited 6/14/2019).

harmful because it may take some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.[27]

48. 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."[28]

49. According to the Federal Trade Commission ("FTC"), identity theft victims must often spend countless hours and large amounts of money repairing the impact to their credit.[29] Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[30]

50. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account – they can also commit various types 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 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, prescription drugs and goods, using fraudulent medical billing in the victim's name, and may even give the victim's personal information to police during an arrest,

[27] *Id.*, p. 9
[28] *Id.*
[29] *See Identity Theft,* Federal Trade Commission, http://www.consumer.ftc.gov/features/feature-0014-identity-theft for lists of what individuals do to recover and monitor their identities. (Last visited 6/14/2019).
[30] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(b)(9). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. §248.201(b)(8).

resulting in an arrest warrant being issued in the victim's name.[31] Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, and other negative effects.

51. 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. Identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs and other Sensitive Information directly on various Internet websites, making the information publicly available. [32]

52. A study by Experian found that the "average total cost" of medical identity theft to an individual 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.[33] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[34] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy.

53. Further, medical databases are particularly high value targets for identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has

[31] *See Identity Theft*, Federal Trade Commission, *available at* http://www.consumer.ftc.gov/features/feature-0014-identity-theft. (Last visited 6/14/2019).
[32] https://www.welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices/. (Last visited 6/14/2019).
[33] *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 6/14/2019).
[34] *Id.*

a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[35] In fact, the medical industry has experienced disproportionately higher instances of computer theft than any other industry.

54. Defendants have caused harm to their patients by failing to prevent hackers from accessing their Sensitive Information. Regardless whether their Sensitive Information is used in a criminal enterprise, its theft significantly increases the risk of their being exploited in ways that would cause economic harm. This decreases the value of their Sensitive Information, and requires them to take efforts to mitigate against that risk.

55. Reimbursement for a financial loss is an important component of recovery for identity theft, but it does not make an individual whole. Victims of identity theft are forced to spend significant time resolving the problems it causes.

56. In addition, there has been an upward trend in data breaches in recent years.[36] The U.S. Department of Health and Human Services, office for Civil Rights, currently lists 487 breaches affecting 500 or more individuals each, in the past 24 months.[37]

57. Defendants knew or should have known that they had an obligation to secure their patients' Sensitive Information because it is highly valuable information.

V. CLASS ACTION ALLEGATIONS

[35] *See Study: Few Aware of Medical Identity Theft Risk*, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm. (Last visited 6/14/2019).
[36] *See Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (Last visited 6/14/2019) ("2018 [has seen] more data breaches reported than any other year since records first started being published.")
[37] U.S. Dept. of Health and Human Services, Office for Civil Rights, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, (Last visited 6/14/2019).

58. Plaintiffs Peter D. Smith and Emily Smith bring this action on behalf of themselves and all others similarly situated pursuant to Fed. R. Civ. P. 23. Plaintiffs seek to represent a Nationwide Class (the "Nationwide Class"), defined as follows:

> All individuals in the United States whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the Data Breach announced by Quest and LabCorp on or around June 3 and June 5, 2019.

59. The members of the proposed Class are so numerous that the joinder of all members is impractical. While the exact numbers of proposed Class members are unknown to Plaintiffs at this time, it is believed to be in the millions.

60. There is a well-defined community of interest among the members of the Class because common questions of law and fact predominate. Plaintiffs' claims are also typical of members of the Class, and Plaintiffs can fairly and adequately represent the interests of the Class.

61. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(3) because it involves questions of law and fact common to the members of the Class that predominate over any questions affecting only individual members, including but not limited to:

(a) Whether Defendants unlawfully used, maintained or disclosed proposed Class members' Sensitive Information;

(b) Whether Defendants unreasonably delayed notifying affected patients of the Data Breach;

(c) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the sensitive nature of the information

compromised in the Data Breach, including, but not limited to Defendants' failure to encrypt the Sensitive Information;

(d) Whether Defendants' conduct was negligent or grossly negligent;

(e) Whether Defendants' conduct was reckless;

(f) Whether Defendants acted willfully and/or with oppression, fraud or malice;

(g) Whether Defendants' conduct constitutes breach of contract;

(h) Whether Plaintiffs and the proposed Class are entitled to damages, civil penalties, punitive damages and/or equitable and injunctive relief.

62. Plaintiffs' claims are typical of those of other proposed Class members because Plaintiffs' Sensitive Information, like that of every proposed Class member, was disclosed by Defendants.

63. Plaintiffs will fairly and adequately represent and protect the interests of the proposed Class.

64. Plaintiffs' counsel is competent and experienced in class action litigation.

65. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all proposed Class members is not practicable, and questions of law and fact common to the proposed Class predominate over any questions affecting only individual members of the proposed Class.

66. The prosecution of separate actions by individual members of the proposed Class would create a risk of inconsistent or varying adjudications with respect to individual members of the proposed Class, which would establish incompatible standards of conduct

for Defendants and would lead to repetitive adjudication of common questions of law and fact.

67. Damages for any individual Class member are likely insufficient to justify the cost of individual litigation, so that, in the absence of class certification, Defendants' violations of the law would go unremedied and Defendants will retain the benefits of their wrongdoing.

68. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(3). The above common questions of law and/or fact predominate over any questions affecting individual members of the proposed Class and a class action is superior to the other available methods for the fair and efficient adjudication of the controversy.

69. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), proposed Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the proposed Class as a whole.

FIRST CLAIM FOR RELIEF

Negligence

(On behalf of Plaintiffs and the Nationwide Class)

70. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

71. Diagnostic Services Defendants required Plaintiffs Peter D. Smith, Emily Smith, and all proposed Class members to submit Sensitive Information to obtain medical services. Diagnostic Services Defendants then provided Plaintiffs' and proposed Class members' Sensitive Information to AMCA.

72. Defendant Quest provided Plaintiffs' and proposed Class members' Sensitive Information to AMCA via Defendant Optum360, while LabCorp provided proposed Class members' Sensitive Information directly to AMCA.

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

74. Defendants had a duty to implement a process by which they could detect a breach of their systems in a reasonably short period of time and to give prompt notice to those affected by a data breach.

75. Defendants owed a duty of care to Plaintiffs and members of the proposed Class to provide security consistent with industry standards and the other laws and requirements discussed above, and to ensure that their systems, networks, and the people responsible for them, adequately protected their patients' Sensitive Information.

76. Defendants' duty to use reasonable security measures resulted from the special relationship between Diagnostic Services Defendants 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 Plaintiffs and the proposed Class members from the harms of a data breach.

77. HIPAA requires Defendants to reasonably protect Sensitive Information 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 Sensitive Information in this case includes protected health information (PHI) within the meaning of HIPAA.

78. Defendants also have 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." The FTC has interpreted the failure to use reasonable measures to protect confidential data to constitute an "unfair practice" under this provision.

79. Defendants' duty to use reasonable care in protecting Sensitive Information also arises pursuant to industry standards, which Defendants are bound by and with which they have agreed to comply.

80. Defendants breached their common law, statutory and other duties and were therefore negligent when they failed to use reasonable measures to protect patients' Sensitive Information, and also when they failed to provide timely notice of the Data Breach.

81. Defendants committed negligent acts and omissions when they:

(a) Failed to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and proposed Class members' Sensitive Information;

(b) Failed to adequately monitor the security of AMCA's networks and systems;

(c) Allowed unauthorized access to Plaintiffs' and proposed Class members' Sensitive Information;

(d) Failed to timely recognize that Plaintiffs' and proposed Class members' Sensitive Information had been compromised; and

(e) Failed to timely warn Plaintiffs and proposed Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

82. Defendants could foresee that their failure to use reasonable measures to protect patients' Sensitive Information and to provide timely notice of the Data Breach would result in injury to Plaintiffs and other proposed Class members. Defendants could foresee the Data Breach, the hackers' unauthorized access, and the resulting injuries to Plaintiffs and proposed Class members.

83. The foreseeable injuries to Plaintiffs and proposed Class members include, but are not limited to:

(a) Ongoing, imminent threat of identity theft crimes, fraud and abuse resulting in monetary loss and economic harm;

(b) Actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm;

(c) Loss of the confidentiality of the stolen Sensitive Information;

(d) Illegal sale of the stolen Sensitive Information on the deep web black market;

(e) Expenses and time spent on credit monitoring and identity theft insurance;

(f) Expenses and time spent monitoring bank statements, credit card statements and credit reports;

(g) Expenses and time spent initiating fraud alerts;

(h) Decreased credit scores and ratings;

(i) Lost work time; and

(j) Other economic and non-economic harm.

84. Plaintiffs seek on their own behalf and on behalf of the proposed Class an order declaring that Defendants' conduct constitutes negligence and awarding damages in an amount to be determined at trial.

SECOND CLAIM FOR RELIEF

Breach of Contract

(On behalf of Plaintiffs and the Nationwide Class)

85. Plaintiffs incorporates by reference all preceding paragraphs as if fully set forth herein.

86. Plaintiffs and proposed Class members entered into contracts with their respective Diagnostic Services Defendants for the provision of diagnostic services.

87. The terms of Diagnostic Services Defendants' Privacy Policies are part of the contracts.

88. Plaintiffs and proposed Class members performed substantially all that was required of them under their contracts with Defendants, or they were excused from doing so.

89. Defendants failed to perform their obligations under the contracts, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs' and proposed Class members' Sensitive Information.

90. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and proposed Class members did not receive the full benefit of the bargain, and instead received diagnostic services that were less valuable than described in their contracts.

Plaintiffs and proposed Class members therefore were damaged in an amount at least equal to the difference in value between that which was promised and Defendants' deficient performance.

91. Also, as a result of Defendants' breach of contract, Plaintiffs and proposed Class members have suffered actual damages resulting from the exposure of their Sensitive Information, and they remain at imminent risk of suffering additional damages in the future.

92. Accordingly, Plaintiffs and proposed Class members have been injured by Defendants' breach of contract and are entitled to damages and/or restitution in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF

Breach of Implied Contract

(On Behalf of Plaintiffs and the Nationwide Class)

93. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

94. Plaintiffs brings this cause of action on behalf of themselves and the proposed Class, to the extent necessary.

95. When Plaintiffs and proposed Class members paid money and provided their Sensitive Information to Defendants in exchange for services, they entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect their Sensitive Information and to notify them timely of its breach or compromise.

96. Defendants solicited and invited prospective patients to provide their Sensitive Information as part of their regular business practices. These patients accepted Defendants' offers and provided their Sensitive Information to them. In entering such implied contracts, Plaintiffs and proposed Class members assumed that Defendants' data security practices and policies were reasonable and consistent with industry standards, and that Defendants would use part of the funds received from Plaintiffs and proposed Class members to pay for adequate and reasonable data security.

97. Plaintiffs and proposed Class members would not have provided and entrusted their Sensitive Information to Defendants in the absence of the implied contracts between them and Defendants to keep it secure.

98. Plaintiffs and proposed Class members fully performed their obligations under their implied contracts with Defendants.

99. Defendants breached their implied contracts with Plaintiffs and proposed Class members by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their Sensitive Information was compromised as a result of the Data Breach.

100. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiffs and proposed Class members sustained actual losses and damages as described herein.

FOURTH CLAIM FOR RELIEF

Unjust Enrichment

(On Behalf of Plaintiffs and the Nationwide Class)

101. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

102. Plaintiffs and the proposed Class members conferred monetary benefit on Defendants. Plaintiffs and the proposed Class members made purchases and paid for goods and services sold by Defendants and provided Defendants with their Sensitive Information for those purchases. Plaintiffs and the proposed Class members would not have made those purchases had they known that Defendants did not provide adequate protection for their Sensitive Information. In exchange for these purchases and payment, Plaintiffs and the proposed Class members bargained for adequate data security for their Sensitive Information.

103. Defendants knew that Plaintiffs and the proposed Class members conferred a benefit on Defendants. Defendants profited from the purchases and used their patients' Sensitive Information for their own business purposes.

104. The payments made for goods and services sold by Defendants should have been used by Defendants, at least in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

105. Defendants failed to properly secure Plaintiffs' and the proposed Class members' Sensitive Information and were thus unjustly enriched by not providing the full benefit of the bargain made with Plaintiffs and the proposed Class members.

106. As a result of Defendants' conduct described herein, Plaintiffs and the proposed Class members suffered actual damages.

107. If Plaintiffs and the proposed Class members had been aware of Defendants' failure to safeguard their Sensitive Information, they would not have purchased Defendants' goods and services.

108. Plaintiffs and the proposed Class members have no adequate remedy at law.

109. Under these circumstances and principles of equity and good conscience, it is unjust for Defendants to retain the benefits that Plaintiffs and the proposed Class members conferred upon them because Defendants failed to use that money to implement the reasonable data privacy and security practices and procedures for which Plaintiffs and the proposed Class members paid.

110. Defendants should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and the proposed Class members proceeds that they unjustly received.

111. In the alternative, Defendants should be compelled to refund the amounts that the Plaintiffs and the proposed Class members overpaid.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on their own behalf and on behalf of proposed Class members, prays for judgment against Defendants as follows:

(a) Certification of the proposed Class;

(b) Appointment of Plaintiffs as Class representatives;

(c) Appointment of the undersigned counsel as counsel for the proposed Class;

(d) Declaration that Defendants' actions described above constitute negligence, violations of HIPAA and the consumer protection laws of Minnesota and other states, breach of contract and implied contract, and unjust enrichment;

(e) Award Plaintiffs and the proposed Class damages as allowed by law;

(f) Award Plaintiffs and the proposed Class injunctive and declaratory relief as allowed by law and/or equity;

(g) Award Plaintiffs and the proposed Class attorneys' fees and costs, as allowed by law and/or equity;

(h) Permit leave to amend this Complaint to conform to the evidence presented at trial; and

(i) Grant such other and further relief as this Court deems necessary, just and proper.

JURY DEMAND

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

Date: July 18, 2019

CHESTNUT CAMBRONNE PA

By /s/ Karl L. Cambronne

Karl L. Cambronne (#14321)
Bryan L. Bleichner (#0326689)
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
kcambronne@chestnutcambronne.com
bbleichner@chestnutcambronne.com

Karen Hanson Riebel
Kate M. Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Andrew N. Friedman
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave NW, Suite 500
Washington, DC 20005
Telephone: (202) 408-4600
afriedman@cohenmilstein.com

ATTORNEYS FOR PLAINTIFFS