Exhibit C21

Andrew J. Schwaba (NC Bar No. 36455)
SCHWABA LAW FIRM
aschwaba@schwabalaw.com
212 South Tryon Street, Suite 1725
Charlotte, NC 28281
(704) 370-0220
(704) 370-0210 (fax)

Edward H. Nicholson, Jr. (NC Bar No. 36123)
NICHOLSON LAW FIRM, P.A.
nicholsonshumaker@att.net
212 South Tryon Street, Suite 1725
Charlotte, NC 28281
(704) 223-2406 (telephone)

Class Counsel

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF NORTH CAROLINA

WESTERN DIVISION

PERNELL THOMAS,

Plaintiff,

v.

RETRIEVAL MASTERS CREDITORS BUREAU INC., d/b/a AMERICAN MEDICAL COLLECTIONS AGENCY, INFORM DIAGNOSTICS INC., LABORATORY CORPORATION OF AMERICA HOLDINGS d/b/a LABCORP

Defendants.

Case No. _____

Assigned to _____

PLAINTIFFS' CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs, Pernell Thomas by his attorneys, makes the following allegations based upon knowledge with respect to his own acts and based upon information and belief with respect to other matters:

I. INTRODUCTION

1. This is a putative class action complaint alleging the Defendants, American Medical Collections Agency, LabCorp, and Inform Diagnostics, negligently, and in violation of the consumer protection statutes of New York, North Carolina and Texas, failed to secure the Personally Identifiable Information ("PII") and Personal Health Information ("PHI") of the Plaintiff and class members.

2. The Defendants informed the Plaintiff and Class Members that AMCA had allowed unauthorized access to the Plaintiff and Class Members PII/PHI by third parties. The unauthorized access allowed third parties access to Plaintiff and Class Members' information including social security numbers, credit card numbers and other bank information, medical history and other personal health information. Defendants' disclosure has harmed the Plaintiff and Class Members which are expected to number thousands of persons.

II. PARTIES

3. Plaintiff Pernell Thomas is a resident of Castalia, North Carolina. He had medical services performed for him by Inform Diagnostics and LabCorp which held his personal identifiable information and personal health information in their database.

4. Defendant, Retrieval Masters Credit Bureau Inc., doing business as, American Medical Collections Agency Inc., ("AMCA") is a corporation with a principal place of business located at 4 Westchester Place, Suite 110, Elmsford, New York 10523. The Defendant, American Medical Collections Agency was contracted by Defendants, Inform Diagnostics Inc. and LabCorp to perform collections services for medical charges related to medical services performed on behalf of the Plaintiff and the proposed class by the Defendants Inform Diagnostics and LabCorp.

5. Defendant, Inform Diagnostics Inc., is a corporation with a principal place of business located at 6655 North MacArthur Avenue in Irving, Texas with a registered agent for service of process CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. The Defendant, Inform Diagnostics, Inc. is a laboratory company performing anatomic pathology services to clinicians in support of patient care on behalf of the Plaintiff and the proposed class, which involved the acquisition and maintenance of the Plaintiff's personal protected health information.

6. Defendant Laboratory Corporation of America Holdings, d/b/a LabCorp is a Delaware corporation with a principal place of business located at 358 South Main Street, Burlington, North Carolina 27215. The Defendant, LabCorp performed medical services on behalf of the Plaintiff and the proposed class, which involved the acquisition and maintenance of the Plaintiff's personal protected health information.

III. JURISDICTION AND VENUE

7. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because the proposed class has more than 100 members, the class contains at least one member of diverse citizenship from Defendants, and the amount in controversy exceeds $5 million.

8. The Court has personal jurisdiction over the Defendants because the Plaintiff resides in this District and the Defendants conduct substantial business in this District, the Plaintiffs provided their personal protected information and the Defendants attempted to collect debts within this District and throughout the State of North Carolina.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1), because the Defendants regularly conduct business in this District. Venue is proper pursuant to 28 U.S.C. § 1391(b)(2), because a substantial part of the transactions at issue occurred in this District. Venue is proper pursuant to 28 U.S.C. § 1391(b)(3), because all Defendants are subject to personal jurisdiction in this District.

IV. FACTUAL BACKGROUND

A. PII/PHI Is A Valuable Property Right.

10. PII/PHI is a valuable property right.[1] In a Federal Trade Commission ("FCC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[2]

11. The value of PII/PHI as a commodity is measurable.[3] "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[4] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market" for several years.

12. Companies recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[5]

---

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

[2] Federal Trade Commission, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), *available at* https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[3] *See* Robert Lowes, Stolen EHR *[Electronic Health Record] Charts Sell for $50 Each on Black Market* (April 28, 2014), *available at* http://www.medscape.com/viewarticle/824192.

[4] *See* Soma, *Corporate Privacy Trend, supra.*

[5] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

13. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

14. PHI is particularly valuable. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[6] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen social security or credit card number.[7]

15. Recognizing the high value that consumers place on their PII/PHI, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the

[6] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013), *available at* https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.

[7] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014) *available at* https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

surrender of their PII/PHI.[8] This business has created a new market for the sale and purchase of this valuable data.[9]

16. Consumers place a high value not only on their PII/PHI, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

17. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[11]

18. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

B. Theft of PII/PHI Has Grave and Lasting Consequences for Victims.

19. Theft of PII/PHI is serious. The United States Government Accountability Office noted in a June, 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a

[8] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) available at https://www.nytimes.com/2010/07/18/business/18unboxed.html.

[9] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) available at https://www.wsj.com/articles/SB10001424052748703529004576160764037920 27.

[10] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), available at https://www.jstor.org/stable/23015560?seq=1#page_scan_tab_contents.

[11] II–Horn, Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at*

https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

person's name.[12] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

20. 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." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[13]

21. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[14] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receive bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[15]

22. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified

---

[12] *See* http:///www.gao.gov/new.items/d07737.pdf.

[13] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[14] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. 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. *Id.*

[15] *See* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

information in medical records that can plague victims' medical and financial lives for years."[16] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[17] "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[18]

23. A report published by the World Privacy Form and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

> Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
>
> - Significant bills for medical goods and services not sought nor received.
> - Issues with insurance, co-pays, and insurance caps.
> - Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
> - Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
> - As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
> - Phantom medical debt collection based on medical billing or other identity information.
> - Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

[16] Pam Dixon, et al., *The Geography of Medical Identity Theft* (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037142815.pdf.

[17] *See* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014).

[18] See Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

A person whose PII/PHI has been compromised may not see any signs of identity theft for years. According to the GAO Report:

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

24. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[19]

25. It is within this context that Plaintiff and the Class Members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

26. Defendants had obligations created by HIPAA, arising from promises made to patients like Plaintiffs and other Class Members, and based on industry standards, to keep the compromised PII/PHI confidential and to protect it from unauthorized disclosures. Class Members provided their PII/PHI to Defendants with the understanding that Defendants and any business partners to whom Defendants disclosed the PII/PHI would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

27. The medical industry is a particularly ripe target for data hackers and cyber criminals as the medical industry has experienced a number of data breaches allowing unauthorized access to patient information, including breaches at Anthem Inc., Excellus Health Plan Inc., and the University of California, Los Angeles Health, which allowed access to millions of persons' PII/PHI.

[19] *See* https://blog.linkedin.com/2016/05/18/protecting-our-members.

C. Defendants Were Obligated to Maintain Reasonable Security Practices for Consumer PHI Data.

28. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal computer 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 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.

29. The FTC has also published a document titled "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.

30. 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.

31. Title II of the Health Insurance Portability and Accountability Act ("HIPAA") (42 U.S.C. § 1301 et seq.) requires the Department of Health and Human Services to establish standards and rules for how PII/PHI should be safeguarded. HIPAA required the Defendants to:

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

b. Adequately protect Plaintiffs' and the Classes' Sensitive Information;

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

d. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, pursuant to 45 C.F.R. § 164.312(a)(1);

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

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

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

32. 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, 15 U.S.C. § 45.

D. Defendants' Security Practices Failed to Secure Consumers' PHI Data and Failed to Follow Their Own Standards.

33. AMCA failed to publish its privacy practices for the security of consumers' PHI.

34. Inform Diagnostics maintained a privacy policy that advised consumers their personal information would never be removed from Inform Diagnostics databases due to technical constraints and the fact that they back up their systems. Inform Diagnostics informed consumers that they had implemented policies, procedures and technologies to address the privacy and security standards, requirements and implications of the rules promulgated pursuant to HIPAA. Inform Diagnostics advised consumers that they use industry standard techniques such as firewall, encryption and intrusion detection. In addition, Inform Diagnostics advised

consumers that they limit employees and contractors' access to personal customer information. Inform Diagnostics advised customers that only employees and contractors who have a business reason to know would have access to personal customer information. Inform Diagnostics represented to customers that they educated their employees about the importance of maintaining the confidentiality of customer information. Finally, Inform Diagnostics advised consumers that they reviewed their security arrangements from time to time as they deemed appropriate.

35. LabCorp advised consumers that they were committed to the protection of their consumers' PHI and would make reasonable efforts to ensure the confidentiality of their PHI as required by statute and regulation. LabCorp advised that they took this obligation seriously. LabCorp advised that they may disclose PHI to business associates who perform billing services and those associates were required to maintain the privacy and confidentiality of consumers' PHI. LabCorp advised consumers that they worked diligently to provide exceptional, quality service to all its clients and is committed to implementing HIPAA.

36. 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.

37. As a result, Defendants knew or should have known that the PII/PHI information that they possessed would be subject to attempts to gain unauthorized access by would-be cyber criminals and hackers, and that insufficient data security practices and systems would result in data breaches and the release of Plaintiff's and Class Members' PII/PHI.

38. In February of 2019, a private monitoring company, Gemini Advisory, identified a cache of approximately 200,000 sets of personal information including names, dates of birth, social security numbers, with some including credit card

numbers and bank account information that were compromised between September 2018 and March of 2019. Gemini Advisory determined it was likely this financial information originated from a data breach of AMCA's computer networks and notified AMCA. When AMCA did not respond, Gemini contacted federal law enforcement, which contacted AMCA directly. On April 8, 2019, AMCA disabled the payment portal suspected of being the hackers' point of entry into AMCA's networks.

39. From August 1, 2018 to March 30, 2019, unauthorized parties were allowed to access the PII/PHI of the Plaintiff and Class Members through the AMCA system, including the social security numbers, bank account and credit card information, and other personal medical information of the Plaintiff and Class Members.

40. According to a form letter sent by Inform Diagnostics to Plaintiff, on July 22, 2019, the Plaintiff and Class Members were informed by Inform Diagnostics that their PII/PHI information had been accessed. According to Inform Diagnostics letter, AMCA notified Inform Diagnostics of the unauthorized access on June 3, 2019.

41. According to a form letter sent by LabCorp to Plaintiff, on July 20, 2019, the Plaintiff and Class Members were informed by LabCorp that their PII/PHI information had been accessed. According to LabCorp's letter, AMCA notified LabCorp of the unauthorized access on May 14, 2019.

42. By allowing the unauthorized access into their data systems, Defendants failed to comply with HIPAA regulations and data safeguards. Defendants' security failures demonstrate 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;

b. Adequately protecting Plaintiffs' and the Classes' Sensitive Information;

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

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).

43. Defendants failed to comply with Section 5 of the Federal Trade Commission Act of 1914, 15 U.S.C. § 45 to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data.

E. It is Well-Established That Data Breaches Lead to Identity Theft.

44. Plaintiffs and other Class Members have been injured by the disclosure of their Sensitive Information in the Data Breach.

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

benefits and incur charges and credit in a person's name.[20] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

46. 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."[21]

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

48. There may be a time lag between when PII/PHI is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft.* Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years.* As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. [22]

49. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but

[20] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited June 4, 2019).

[21] *Id.* at 2, 9

[22] *Id*. at 29 (emphasis supplied).

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 in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name. [23]

50. PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other PII/PHI directly on various Internet websites making the information publicly available.

51. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[24]

52. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole. Medical databases are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1." [25] In fact, the medical

---

[23] *See Federal Trade Commission*, Warning Signs of Identify Theft, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited June 4, 2019).

[24] *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 June 4, 2019).

[25] *See* Study; Few Aware of Medical Identity Theft Risk, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 4, 2019).

industry has experienced disproportionally higher instances of computer theft than any other industry.

V. CLASS ACTION ALLEGATIONS

53. Plaintiffs incorporate all previous allegations as though fully set forth herein.

54. Plaintiffs bring this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

55. Plaintiffs bring this case individually and as a class action pursuant to Rules 23(b)(1), 23(b)(2) and/or 23(c)(4) of the Federal Rules of Civil Procedure on behalf of a proposed class, as follows:

Nationwide Class: All individuals in the United States whose personal information was provided to AMCA by Inform Diagnostics and/or LabCorp, and was compromised as a result of the AMCA data breach.

North Carolina Subclass: All individuals residing in North Carolina whose personal information was provided to AMCA by Inform Diagnostics and/or LabCorp and was compromised as a result of the AMCA data breach.

Texas Subclass: All individuals residing in Texas whose personal information was provided to AMCA by Inform Diagnostics and/or LabCorp, and was compromised as a result of the AMCA data breach.

Excluded from the proposed classes are Defendants, any officer, director, employee or agent of the Defendants; an entity in which Defendants have a controlling interest; any affiliate, parent or subsidiary of the Defendants; any successor or assigns of the Defendants; any employee of the law firms or counsel in this action; and any judge to whom this case is assigned, her or his staff, and close personal family members.

56. The members of the class are similarly situated to Plaintiffs.

57. **Numerosity**: The class consists of thousands, and possibly millions of persons whose PII/PHI was granted unauthorized access in the AMCA data breach,

making joinder of each individual impracticable.

58. **Commonality**: Common questions of law and fact exist with respect to the class. They include:

a. Whether Defendants took reasonable measures to safeguard the PII/PHI of the Plaintiff and Class Members;

b. Whether Defendants Inform Diagnostics and/or LabCorp properly researched, investigated, hired and supervised AMCA to determine whether AMCA maintained adequate data security safeguards;

c. Whether Defendants breached their duty as it allowed their databases, computer systems, and other patient information repository to be compromised;

d. Whether Defendants complied with federal and state privacy laws, including HIPAA and others;

e. Whether Defendants breached their contract with Plaintiff and Class Members to secure Plaintiffs and Class Members PII/PHI;

f. Whether Defendants violated state consumer protection laws, by failing to safeguard Plaintiff and Class Members PII/PHI;

g. Whether Defendants failed to timely and adequately inform Plaintiff and Class Members of a data breach;

h. Whether Plaintiff and Class Members are entitled to damages including statutory penalties, restitution, compensation and injunctive relief;

59. The common issues of law and fact of the class members are very similar and are the most significant issues in the case. These common issues predominate over any individual issues, and they can be resolved for all members of the class in one action.

60. **Typicality**: Plaintiffs' claims are typical of the claims of the Class Members and the factual and legal bases for the claims are similar. Plaintiff and Class

Members were notified by form letter from the Defendants that their PII/PHI had been compromised, have sustained similar injuries and allege claims based on similar, and identical failures by the Defendants.

61. **Adequacy**: Plaintiffs will fairly and adequately represent the interests of the Class in that:

a. Plaintiffs' interests do not conflict with those of the Class Members. Plaintiffs do not have any relationship with Defendants except as a patient of the medical providers identified herein as described.

b. Plaintiffs and their attorneys have adequate legal and financial resources to prosecute this action diligently. Plaintiffs' counsel can advance the costs of this action.

c. Plaintiffs' attorneys are competent and experienced in class action litigation.

62. A class action is the superior method for adjudicating the claims asserted herein, and a class action will provide a fair and efficient method of adjudicating this controversy. The management of this litigation as a class action will not present any undue difficulties.

63. The claims asserted herein are "negative value" claims (it would cost more to litigate them individually than could be recovered individually), making prosecution of the claims in separate actions by individual members of the class financially impracticable.

64. Separate prosecution of the claims would also be burdensome and inefficient for counsel and the Court.

VII. CAUSES OF ACTION

COUNT I –NEGLIGENCE

(On Behalf of Plaintiff and Nationwide Class)

65. Plaintiffs incorporate the previous allegations as though fully set forth herein.

66. Plaintiffs reallege and incorporate by reference all preceding factual allegations.

67. Quest required Plaintiffs and Class Members to submit non-public Personal Information to obtain medical services, which Quest provided to AMCA for billing purposes.

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

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

70. Defendants also owed a duty of care to Plaintiffs and members of the Classes to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them adequately protected their customers' Sensitive Information.

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

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

confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

73. In addition, Defendants had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

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

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

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

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class members' Sensitive Information;
b. failing to adequately monitor the security of AMCA's network and systems;
c. allowing unauthorized access to Plaintiffs' and Class Members' Sensitive Information;
d. failing to recognize in a timely manner that Plaintiffs' and other Class Members' Sensitive Information had been compromised; and
e. failing to warn Plaintiffs and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

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

78. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiffs and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

79. Accordingly, Plaintiffs, individually and on behalf of all those similarly situated, seek an order declaring that Defendants' conduct constitutes negligence and awarding damages in an amount to be determined at trial.

COUNT II –VIOLATIONS OF N.Y. GEN. BUS. LAW § 349

(On Behalf of Plaintiff and the Nationwide Class)

80. Plaintiffs incorporate the allegations above as though fully set forth herein.

81. Defendants, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

a. Defendants failed to enact adequate privacy and security measures to protect the Class Members' Sensitive from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendants failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Defendants knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

d. Defendants omitted, suppressed, and concealed the material fact of Defendants' reliance on, and inadequacy of, AMCA's security protections;

e. Defendants knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information, including but not limited to duties imposed by HIPAA; and

f. Defendants failed to disclose the Data Breach to the victims in a timely and accurate manner, in violation of the duties imposed by, inter alia, N.Y. Gen Bus. Law § 899-aa(2).

82. As a direct and proximate result of Defendants' practices, Plaintiff and other Class members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial and medical accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Information.

83. The above unfair and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts

caused substantial injury to Plaintiff and other Class Members that they could not reasonably avoid, which outweighed any benefits to consumers or to competition.

84. Defendants knew or should have known that AMCA's computer systems and data security practices were inadequate to safeguard Sensitive Information entrusted to it, and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-referenced unfair practices and deceptive acts were negligent, knowing and willful.

85. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs. The amount of such damages is to be determined at trial but will not be less than $50.00 per violation.

86. Plaintiff and Class Members seek to enjoin such unlawful deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court enjoins Defendants' unlawful, deceptive actions in that Defendants will continue to fail to protect Sensitive Information entrusted to them, as detailed herein.

87. Plaintiff and Class Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendant from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

COUNT III – BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Nationwide Class)

88. Plaintiffs incorporate the previous allegations as though fully set forth herein.

89. When Plaintiff and Class members paid money and provided their PII/PHI to Defendants in exchange for services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such

information and to timely and accurately notify them if their data had been breached and compromised.

90. Defendants solicited and invited prospective clients and other consumers to provide their PII/PHI as part of its regular business practices. These individuals accepted Defendants' offers and provided their PII/PHI to Defendants. In entering into such implied contracts, Plaintiffs and the Class 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 the Class to pay for adequate and reasonable data security practices.

91. Plaintiff and the Class Members would not have provided and entrusted their PII/PHI to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

92. Plaintiff and the Class Members fully performed their obligations under the implied contracts with Defendants.

93. Defendants breached their implied contracts with Plaintiff and the Class Members by failing to safeguard and protect their PII/PHI and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

94. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiff and the Class Members sustained actual losses and damages as described herein.

COUNT IV – UNFAIR AND DECEPTIVE TRADE PRACTICES NORTH CAROLINA – CHAPTER 75

(On Behalf of Plaintiff and the North Carolina Subclass)

95. Plaintiff re-alleges and incorporates herein by reference the allegations set forth above as though fully set forth herein.

96. At all times relevant herein, the defendants provided commercial billing services in the State of North Carolina. As such, their activities and practices were

governed by the North Carolina Unfair and Deceptive Trade Practices Act, codified at N.C. G.S. § 75-1.1 et seq.

97. The Defendants committed an unfair or deceptive act or practice in the sale, bill processing, and billing payments for the Plaintiff's medical treatment.

98. The defendants violated the North Carolina Unfair and Deceptive Trade Practices Act, N.C. G.S. § 75-1.1 in that they:

a. Violated the HIPAA, codified at 42 U.S.C. § 1303 *et seq*.;

b. They did not adequately safeguard consumers PII/PHI;

c. They failed to properly monitor data security systems for existing intrusions;

d. They failed to inspect and ensure that contractors and vendors entrusted with PII/PHI were employing reasonable data security practices;

e. They failed to notify Plaintiff and North Carolina Subclass members that their PII/PHI had been exposed to unauthorized persons as they were obligated to do pursuant to N.C. G.S. §§ 75-61, 75-65;

f. They failed to comply with Section 5 of the FTC Act;

h. They failed to comply with N.C.G.S. § 8-53 et seq.

99. The Defendants' commercial collections services and handling of the Plaintiff's PII/PHI affected commerce.

100. The defendants' violation of the North Carolina Unfair and Deceptive Trad Practices Act, N.C. G.S. § 75-1.1, caused the plaintiff the injuries and damages as alleged more fully below.

COUNT V – VIOLATIONS OF TEX. BUS. & COM. CODE § 17.45

(On Behalf of Plaintiff and the Texas Subclass for Inform Diagnostics Customers)

101. Defendants are "persons" as defined by Tex. Bus. & Com. Code § 17.45(3).

102. Mr. Thomas and the Texas Subclass members are "consumers" as

defined by Tex. Bus. & Com. Code § 17.45(4).

103. Defendant, Inform Diagnostics, engaged in trade or commerce within the meaning of Tex. Bus. & Com. Code § 17.45(6), in that they engaged in trade and commerce that directly or indirectly affected the people of Texas, and they advertised, offered for sale, sold, leased, or distributed goods or services within the meaning of the statute.

104. Defendant, Inform Diagnostics, engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b) including:

a. Causing confusion or misunderstanding as to the certification of goods or services;

b. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

c. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and advertising goods or services with intent not to sell them as advertised;

d. Advertising goods or services with intent not to sell them as advertised;

e. Failing to disclose information concerning goods or services which was known at the time of the transaction where such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

105. Defendants false, misleading and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Mr. Thomas' and the Texas subclass members' personal information, which was a direct and proximate cause of the Defendant's data breach;

b. Failing to identify foreseeable security and privacy risks, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to

the security and privacy of Mr. Thomas and Texas Subclass members' personal information, including duties imposed by the HIPAA, FTC Act, 15 U.S.C. § 45 et seq., and Texas data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the data breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Mr. Thomas' and Texas Subclass members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would protect the privacy and confidentiality of Mr. Thomas' and Texas Subclass members' personal information, including duties imposed by the HIPAA, FTC Act, 15 U.S.C. § 45 et seq., and Texas data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Mr. Thomas's and the Texas Subclass members personal information; and

g. Omitting, suppressing and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Mr. Thomas' and Texas Subclass members' personal information, including duties imposed by the HIPAA, the FTC Act, 15 U.S.C. § 45 et seq., and Texas data security statute, Tex. Bus. & Com. Code § 521.052.

106. Defendants intended to mislead Mr. Thomas and Texas Subclass members and induce them to rely on the misrepresentations and omissions.

107. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' personal information.

108. Mr. Thomas and Texas Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

109. Defendants had a duty to disclose the above facts due to the

circumstances of this case, the sensitivity and amount of personal information in their possession, and the generally accepted professional standards in the industry. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Mr. Thomas and the Texas Subclass, and Defendants because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from their:

a. Possession of exclusive knowledge regarding the security of the data in their systems;

b. Active concealment of the state of their security controls; and/or

c. Incomplete representations about the security and integrity of their computer and data systems, while purposefully withholding material facts from Mr. Thomas and the Texas Subclass that contradicted these representations.

110. Consumers, including Mr. Thomas and the Texas Subclass members, lacked knowledge about deficiencies in Defendants' data security because this information was known exclusively by Defendants. Consumers also lacked the ability, experience, or capacity to secure the personal information in Defendants' possession or to fully protect their interests with regard to their data. Mr. Thomas and the Texas Subclass members lack expertise in information security matters and do not have access to Defendants' systems in order to evaluate its security controls. Defendants took advantage of their special skill and access to personal information to hide their inability to protect the security and confidentiality of Mr. Thomas and the Texas Subclass members' personal information.

111. Defendants intended to take advantage of consumers' lack of knowledge, ability, experience or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Defendants' conduct is glaringly noticeable, flagrant, complete, and unmitigated. The data breach, which resulted from Defendant's business acts and practices, exposed

Mr. Thomas and the Texas Subclass members to a wholly unwarranted risk to the safety of their personal information and the security of their identity and credit, and worked a substantial hardship on a significant and unprecedented number of consumers, Mr. Thomas and the Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

112. Defendants acted intentionally, knowingly, and maliciously to violate Texas' Deceptive Trade Practices – Consumer Protection Act, and recklessly disregarded Mr. Thomas' and Texas Subclass members' rights.

113. As a direct and proximate result of Defendants' deceptive acts and practices, Mr. Thomas and Texas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money and property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased risk of fraud and identity theft; loss of the benefits of their bargains with Defendants; and loss of value of their personal information. Defendants' deceptive acts or practices were a producing cause of Mr. Thomas' and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

114. Defendants' violations present a continuing risk to Mr. Thomas and the Texas Subclass members as well as to the general public.

115. Mr. Thomas and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

CONCLUSION

WHEREFORE, Plaintiff, on behalf of himself and Class members, prays for relief as follows:

A. Certification of the action as a Class Action pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiffs as Class Representatives and their counsel of record as Class Counsel;

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;

C. That acts alleged herein be adjudged and decreed to constitute negligence and amount to violations of HIPAA, Section 5 of the FTC, and the consumer protection laws of New York, North Carolina and Texas;

D. A judgment against Defendants for the damages sustained by Plaintiffs and the Classes defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

E. By awarding Plaintiffs and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

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

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

REQUEST FOR JURY TRIAL

Plaintiffs request a trial by jury on all issues.

Dated this 13th day of August, 2019.

SCHWABA LAW FIRM

s/ Andrew J. Schwaba
Andrew J. Schwaba
NC Bar No.: 36455
212 South Tryon Street
Suite 1725
Charlotte, NC 28281
(704) 370-0220
(704) 370-0210 (fax)

aschwaba@schwabalaw.com

NICHOLSON LAW FIRM, P.A.

s/ Edward H. Nicholson, Jr.
Edward H. Nicholson, Jr.
NC Bar No. 36123
212 South Tryon Street
Suite 1725
Charlotte, NC 28281
(704) 223-2406 (telephone)
nicholsonshumaker@att.net

Attorneys for Plaintiffs