BEFORE THE UNITED STATES JUDICIAL PANEL ON
MULTI-DISTRICT LITIGATION

In re: American Medical Collection Agency Data Breach Litigation	MDL No.

MOTION OF PLAINTIFF PAULA WORTHEY FOR TRANSFER AND CENTRALIZATION PURSUANT TO 28 U.S.C. § 1407

In accordance with 28 U.S.C. § 1407, Plaintiff Paula Worthey ("Plaintiff") respectfully moves the Judicial Panel on Multidistrict Litigation for an order transferring and centralizing the Actions listed in the Schedule of Actions (attached hereto) to the United States District Court for the Southern District of New York, before the Honorable Nelson S. Roman. In support of this motion, Plaintiff incorporates by reference the accompanying memorandum of law and aver the following:

1. At the time of filing, this motion involves: *Worthey v. American Medical Collection Agency, Inc. et al.*, Case No. 7:19-cv-05210 (S.D.N.Y.), *Gutierrez v. Am. Medical Collection Agency, Inc., et al.*, Case No. 7:19-cv-05212 (S.D.N.Y.), and *Marler v. Quest Diagnostics, Inc., et al.*, Case No. 8:19-cv-01091 (C.D. Cal.) (collectively, the "Actions").

2. The Actions involve common questions of fact that are sufficiently numerous and complex to warrant centralization. All of the cases are premised on similar factual allegations involving the failure of Defendants American Medical Collection Agency, Inc. ("AMCA"), Optum360 Services, Inc. ("Optum360"), and Quest Diagnostics Incorporated ("Quest") (collectively, "Defendants") to protect the confidential information of millions of patients — including financial information, medical information, personal information, and/or other health information protected by the Health Insurance Portability and Accountability Act of 1996

(collectively, "Sensitive Information"). Each of these actions involve the same putative nationwide and California-based class definitions, and bring nearly identical causes of action.[1] In each case, the court will be asked to determine substantially similar factual issues. Each of these actions is a putative class action that seeks to represent persons who had Sensitive Information maintained on the AMCA systems that was compromised in the data breach announced by Quest on June 3, 2019.

3. All of the Actions are in their infancy. No Defendant has answered the Complaint or otherwise appeared in any of the Actions.

4. Discovery in each case will be substantially identical because many allegations, parties, and witnesses will be nearly identical. Discovery as to many issues common to all the plaintiffs can and should be centralized in a single proceeding, to avoid the inefficiencies and duplication of efforts likely to arise with the Actions pending in different districts.

5. Centralization will prevent duplicative discovery, eliminate the possibility of inconsistent pretrial rulings (particularly on class action issues), conserve judicial resources, reduce the costs of litigation, minimize the inconvenience to the parties and witnesses, and allow the Actions to proceed efficiently to trial. Centralization will also provide a single forum to which future tag-along actions may be transferred to streamline subsequent proceedings and promote judicial economy. Further, centralization will result in development of a consistent law of the case and the fair and economical adjudication of the Actions.

---

[1] Each case includes causes of action for: negligence; breach of implied contract; violation of California's Confidential Medical Information Act, Cal. Civ. Code §§ 56 *et seq.*; violation of the New York General Business Law § 349; violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*; and violation of California's Customer Records Act, Cal. Civ. Code §§ 1798.81 *et seq.* The *Marler* action includes those claims, as well as claims for breach of contract; violation of California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.*; unjust enrichment; and invasion of privacy claims.

6. For these reasons, transfer and centralization of these actions will promote the convenience of the parties and witnesses and the just and efficient conduct of the Actions pursuant to 28 U.S.C. § 1407.

7. Plaintiff respectfully submits that the Panel should enter an order transferring the Actions, as well as any future tag-along actions, to the Southern District of New York, in White Plains, for centralization of pretrial proceedings before Judge Nelson S. Roman. The Southern District of New York is the superior forum because it has a judiciary that is well-experienced with such multi-district proceedings, and is where AMCA and Quest — apparently the primary defendants — are headquartered. Judge Roman currently presides over no MDL proceedings.

8. WHEREFORE, Plaintiff respectfully requests the Panel to order the transfer and centralization of the Actions listed in the Schedule of Actions and any future tag-along actions to the Southern District of New York, before Judge Nelson S. Roman.

This motion is based on the filed Memorandum in support of this motion, the filed pleadings and papers, and any such matters as may be presented to the Panel at the time of the hearing.

Respectfully submitted,

Dated: June 4, 2019

AHDOOT & WOLFSON, PC

/s/ Tina Wolfson

Tina Wolfson
twolfson@ahdootwolfson.com
Brad King
bking@ahdootwolfson.com
Theodore W. Maya
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
45 Main Street, Suite 528
Brooklyn, NY 11201
Tel: 917-336-0171
Fax: 917-336-0177

Russell Yankwitt
russell@yankwitt.com
Michael H. Reed
michael@yankwitt.com
YANKWITT LLP
140 Grand Street
Suite 705
White Plains, NY 10601
Tel: 914-686-1500
Fax: 914-487-5000

Counsel for Plaintiff
and the Putative Classes

BEFORE THE UNITED STATES JUDICIAL PANEL ON
MULTI-DISTRICT LITIGATION

In re: American Medical Collection Agency Data Breach Litigation	MDL No.

MEMORANDUM OF LAW IN SUPPORT OF MOTION OF PLAINTIFF PAULA WORTHEY FOR TRANSFER AND CENTRALIZATION PURSUANT TO 28 U.S.C. § 1407

Pursuant to 28 U.S.C. § 1407 and the Rules of Procedure of the Judicial Panel on Multidistrict Litigation, Plaintiff Paula Worthey ("Plaintiff") respectfully submits this Memorandum of Law in Support of her Motion for Transfer and Centralization of all currently filed federal cases ("Actions") arising out of the Data Breach at issue, and any subsequent "tag along" cases involving similar claims, to the Southern District of New York, before the Honorable Nelson S. Roman.

I. INTRODUCTION

This litigation involves a common data breach announced on or around June 3, 2019 (the "Data Breach"). Plaintiffs in these related cases allege that Defendants American Medical Collection Agency, Inc. ("AMCA"), Optum360 Services, Inc. ("Optum360"), and Quest Diagnostics Incorporated ("Quest") (collectively, "Defendants") failed to protect the confidential information of millions of patients — including their financial information (e.g., credit card numbers and bank account information), medical information, personal information (e.g., Social Security Numbers), and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, "Sensitive Information").

On June 3, 2019, Quest publicly admitted in a filing with the Securities and Exchange Commission ("SEC") that: "On May 14, 2019, American Medical Collection Agency ("AMCA"), a billing collections vendor, notified Quest . . . and Optum360 LLC, [Quest's] revenue cycle management provider," of the massive Data Breach compromising the Sensitive Information of 11.9 million Quest patients, and most likely others (the "Data Breach"). Quest Form 8-K, June 3, 2019. Quest's SEC filing further disclosed that, "between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself[,] . . . include[ing] financial information (e.g., credit card numbers and bank account information), medical information[,] and other personal information (e.g., Social Security Numbers)." Although Quest knew of the Data Breach at least as of May 14, 2019, and AMCA knew of it even earlier, neither took any steps to notify patients whose information was affected until June 3, 2019, at which point Quest only did so through an SEC filing.

Each of the Actions is a putative class action, and each is filed on behalf of a virtually identical nationwide class and California sub-class. *See Worthey v. American Medical Collection Agency, Inc. et al.*, Case No. 7:19-cv-05210 (S.D.N.Y.), Complaint ¶ 29; *Gutierrez v. Am. Medical Collection Agency, Inc., et al.*, Case No. 7:19-cv-05212 (S.D.N.Y.), Complaint ¶ 29; and *Marler v. Quest Diagnostics, Inc., et al.*, Case No. 8:19-cv-01091 (C.D. Cal.), Complaint ¶¶ 64-65. As previously discussed, each action alleges a common failure to protect Plaintiffs' Sensitive Information resulting in the Data Breach announced by Quest on or around June 3, 2019.

Plaintiff is not aware of any other cases being filed on behalf of similarly situated consumers. However, based on the scope of the announced Data Breach, Plaintiff does anticipate

additional cases will be filed nationwide. All such Actions are in their infancy. None of the Defendants have answered the Complaint or otherwise appeared in the Actions.

Based on the numerous common questions of fact involved in the Actions, the compelling need to establish uniform and consistent standards in conducting pretrial discovery and motion practice, and because the most logical and convenient location for these proceedings is the Southern District of New York, Plaintiff respectfully requests coordinated proceedings there.

II. BACKGROUND

This motion for transfer involves three actions pending in two different federal Districts[1] asserting common factual allegation and involving overlapping claims, classes, and legal issues. Based on the extensive press coverage of the Data Breach, Plaintiff expects additional actions to be filed in the federal courts alleging similar claims, on behalf of similar classes.

A. Plaintiffs

All plaintiffs in the pending Actions have filed civil actions arising from Quest's recent disclosure of a massive breach affecting AMCA's systems that compromised the Sensitive Information of at least 11.9 million Quest patients. The Actions are pursued on behalf of all persons whose Sensitive Information was compromised in the Data Breach.

Each of these pending federal cases presents a common core of facts, in that each (i) alleges that plaintiffs' Sensitive Information was disclosed during the Data Breach; (ii) asserts injury and damages arising from Defendants' wrongful conduct; and (iii) alleges the same or similar conduct by Defendants. Indeed, the factual allegations in plaintiffs' complaints are nearly identical in numerous critical respects.

[1] *See* Schedule of Actions, attached, for a complete listing of the Actions.

B. Defendants

Defendant AMCA is a New York corporation with its principal place of business in Elmsford, New York, in the Southern District of New York. Defendant Quest is a Delaware corporation with its principal place of business in Secaucus, New Jersey. Based on information and belief, Defendant Optum360 is a Delaware corporation with its principal place of business in Eden Praire, Minnesota.

C. Status of the Actions

Plaintiffs filed the pending federal actions in New York and California, on the same day as Quest's announcement of the Data Breach. Given the infancy of these cases, none of the plaintiffs have been permitted to conduct discovery, or any other actions that would move the matters along towards trial such that transfer would be unduly prejudicial or inefficient. These Actions are in the earliest procedural stage — no defendant has answered or otherwise appeared — and, accordingly, it is a convenient time to coordinate the Actions.

III. ARGUMENT

The Actions listed in the attached Schedule of Actions name AMCA, Optum360, and Quest as the only three Defendants. There also is substantial overlap between the causes of action: Each case includes causes of action for: negligence; breach of implied contract; violation of California's Confidential Medical Information Act, Cal. Civ. Code §§ 56 *et seq.*; violation of the New York General Business Law § 349; violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*; and violation of California's Customer Records Act, Cal. Civ. Code §§ 1798.81 *et seq.* The *Marler* action includes those claims, as well as claims for breach of contract; violation of California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.*; unjust enrichment; and invasion of privacy claims.

The Actions all involve common issues of fact and a common Data Breach, such that centralization will promote the convenience of the parties and witnesses and the just and efficient conduct of the litigation. *See* 28 U.S.C. § 1407. Transfer and centralization will mitigate the possibility of inconsistent rulings, including rulings regarding class certification, and will promote judicial economy by providing a single forum to which future tag-along actions can be transferred. Accordingly, Plaintiff respectfully moves this Panel for transfer to the Southern District of New York, the most favorable district for centralization, before Judge Roman, a capable and experienced jurist of the highest caliber.

A. These Actions and any Tag-Along Actions Are Appropriate for Transfer and Centralization Under 28 U.S.C. § 1407(A)

Transfer and centralization is permitted if civil actions pending in different districts "involv[e] one or more common questions of fact" and this Panel determines that transfer will further "the convenience of parties and witnesses and will promote the just and efficient conduct of such actions." 28 U.S.C. § 1407(a). "The objective of transfer is to eliminate duplication in discovery, avoid conflicting rulings and schedules, reduce litigation cost, and save the time and effort of the parties, the attorneys, the witnesses, and the courts." *Manual for Complex Litigation*, § 20.131 (4th ed. 2004). Transfer and centralization for pretrial proceedings would achieve those objectives in the instant litigation, and therefore are appropriate here.

i. The Actions Involve Common, Numerous, and Complex Questions of Fact

The first element of the Section 1407 transfer analysis is whether there are one or more common questions of fact. *See* 28 U.S.C. § 1407. The statute, however, does not require a "complete identity or even [a] majority" of common questions of fact to justify transfer. *In re Zyprexa Prods. Liab. Litig.*, 314 F. Supp. 2d 1380, 1381 (J.P.M.L. 2004).

Here, there is no question that these cases share a common core of operative factual allegations. The Actions are based upon identical facts concerning identical conduct by Defendants. The factual questions common to the actions are numerous and complex, including:

- Whether Defendants' data security systems prior to the Data Breach met the requirements of laws including, for instance, HIPAA;
- Whether Defendants' data security systems prior to the Data Breach met industry standards;
- Whether Plaintiff's and other Class members' Sensitive Information was compromised in the Data Breach; and
- Whether Plaintiff's and other Class members are entitled to damages as a result of Defendants' conduct.

In addition, both actions rely upon similar legal theories of recovery. These theories include: negligence; breach of implied contract; violation of California's Confidential Medical Information Act, Cal. Civ. Code §§ 56 *et seq.*; violation of the New York General Business Law § 349; violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*; and violation of California's Customer Records Act, Cal. Civ. Code §§ 1798.81 *et seq.* Thus, the lawsuits share related underlying legal theories of liability, each turning on the failure of Defendants to prevent the Data Breach. As the Panel previously has stated, "the presence of additional or differing legal theories is not significant when the actions still arise from a common factual core . . . ." *In re Oxycontin Antitrust Litig.*, 542 F. Supp. 2d 1359, 1360 (J.P.M.L. 2008).

Because numerous common issues of fact exist among these Actions, the pending actions clearly satisfy the first element of the transfer analysis under Section 1407.

ii. MDL Transfer and Centralization Will Further the Convenience of the Parties and the Witnesses.

Resolution of these common issues in a single forum would further the convenience of all parties and witnesses. *See* 28 U.S.C. § 1407(a). Because all Actions involve similar allegations and factual questions, the plaintiffs in the actions will require depositions of the same persons and discovery of the same documents. Defendants likely will raise the same discovery objections and seek the same protective orders or privileges in each case. Absent centralization and transfer, all parties will be subjected to duplicative discovery and witnesses will face multiple, redundant depositions. *See, e.g., In re Pilot Flying J Fuel Rebate Contract Litigation (No. 11)*, 11 F. Supp. 3d 1351, 1352 (J.P.M.L. 2014) ("Centralization will avoid repetitive depositions of [the defendant's] officers and employees and duplicative document discovery regarding the alleged scheme"); *In re Uranium Indus. Antitrust Litig.*, 458 F. Supp. 1223, 1230 (J.P.M.L. 1978) ("[Plaintiffs] will have to depose many of the same witnesses, examine many of the same documents, and make many similar pretrial motions in order to prove their . . . allegations. The benefits of having a single judge supervise this pretrial activity are obvious.").

Absent transfer, the federal court system will be forced to administer — and Defendants will be compelled to defend — these related actions across multiple venues, all proceeding on potentially different pretrial schedules and subject to different judicial decision-making and local procedural requirements. Moreover, each plaintiff will be required to monitor and possibly participate in each of the other similar actions to ensure that Defendants do not provide inconsistent or misleading information. Many of the same pretrial disputes are likely to arise in each action. Likewise, due to the similar causes of action in each complaint, Defendants will likely assert the same defenses, as well as file motions to dismiss and summary judgment on the same claims based on the same arguments in each action.

None of the pending cases have progressed to the point where efficiencies will be forfeited through transfer to an MDL proceeding. This Panel has routinely recognized that consolidating litigation in one court benefits *both* plaintiffs and defendants. For example, pretrial transfer would reduce discovery delays and costs for plaintiffs, and permit plaintiffs' counsel to coordinate their efforts and share the pretrial workload. *In re Phenylpropanolamine (PPA) Prods. Liab. Litig.*, 173 F. Supp. 2d 1377, 1379 (2001) ("And it is most logical to assume that prudent counsel will combine their forces and apportion their workload in order to streamline the efforts of the parties and witnesses, their counsel and the judiciary, thereby effectuating an overall savings of cost and a minimum of inconvenience to all concerned."); *In re Baldwin-United Corp. Litigation*, 581 F. Supp. 739, 741 (J.P.M.L. 1984) (same). As for Defendants, national or "generic" expert depositions will be coordinated, document production will be centralized, and travel for its current and former employees will be minimized, since it will only have to appear in one location rather than multiple districts around the country.

While Plaintiff anticipates there will be additional case filings, even the current level of litigation would benefit from transfer and coordinated proceedings, given the allegations of these complaints. *See In re First Nat'l Collection Bureau, Inc., Tel. Consumer Prof. Act (TCPA) Litig.*, 11 F. Supp. 3d 1353, 1354 (J.P.M.L. 2014) ("Although there are relatively few parties and actions at present, efficiencies can be gained from having these actions proceed in a single district," such as "eliminat[ing] duplicative discovery; prevent[ing] inconsistent pretrial rulings . . . and conserv[ing] the resources of the parties, their counsel and the judiciary."); *In re: Zurn Pex Plumbing Products Liability Litig.*, 572 F.Supp.2d 1380, 1381 (J.P.M.L. 2008) (granting transfer and consolidation of three cases and six potential tag-alongs because of the

"overlapping and, often, nearly identical factual allegations that will likely require duplicative discovery and motion practice).

Transfer also will reduce the burden on the parties by allowing more efficient and centralized divisions of workload among the attorneys already involved in this litigation, as well as those who join later. Plaintiffs themselves will reap efficiencies from being able to divide up the management and conduct of the litigation as part of a unified MDL process through a plaintiffs' steering committee or similar mechanism, instead of each plaintiffs' firm separately litigating its own cases on distinct and parallel tracks. *In re Phenylpropanolamine (PPA) Prods. Liab. Litig.*, 173 F. Supp. 2d at 1379; *In re Tylenol Mktg., Sales Pracs. and Prods. Liab. Litig.*, 936 F. Supp. 2d at 1379 ("Centralization will ... conserve the resources of the parties, their counsel, and the judiciary.").

In sum, transfer of these actions would serve the convenience of the parties and eliminate duplicative discovery, saving the parties-and the courts significant time, effort, and money.

B. Transfer and centralization Will Promote the Just and Efficient Conduct of These Actions

Centralization is necessary to prevent inconsistent pretrial rulings on many central issues, which would present significant problems due to the substantial consistency in factual and legal allegations among all Actions. *See In re: Lumber Liquidators Chinese-Manufactured Flooring Products Mktg., Sales Practices and Products Liability Litig.*, 109 F. Supp. 3d at 1383 ("Centralization will . . . avoid inconsistent pretrial rulings (including on issues of class certification and *Daubert* motion practice) . . . .").

The prospect of inconsistent rulings also encourages forum and judge shopping (including, for example, manipulation of non-congruent discovery limits, approaches to

electronically stored information, and protective order issues). By contrast, a single MDL judge coordinating pretrial discovery and ruling on pretrial motions in all of these federal cases at once will help reduce witness inconvenience, the cumulative burden on the courts, and the litigation's overall expense, as well as minimizing this potential for conflicting rulings. *In re: Xarelto (Rivaroxaban) Prods. Liab. Litig.*, 65 F. Supp. 3d 1402, 1405 (J.P.M.L. 2014) ("Issues concerning the development, manufacture, regulatory approval, labeling, and marketing of Xarelto thus are common to all actions. Centralization will eliminate duplicative discovery; prevent inconsistent pretrial rulings; and conserve the resources of the parties, their counsel and the judiciary."); *In re Tylenol Mktg., Sales Pracs. and Prods. Liab. Litig.*, 936 F. Supp. 2d at 1379 ("Centralization will ... prevent inconsistent pretrial rulings (on Daubert issues and other matters)....").

Centralization will mitigate these problems by enabling a single judge to manage discovery and the parties to coordinate their efforts. This will reduce litigation costs and minimize inconvenience to the parties and witnesses, to the benefit of litigants, third parties, and the courts. *See In re Enfamil Lipil Mktg. and Sales Practices Litig.*, 764 F. Supp. 2d 1356, 1357 (J.P.M.L. 2011) ("Centralizing the actions will allow for the efficient resolution of common issues and prevent unnecessary or duplicative pretrial burdens from being placed on the common parties and witnesses."); *In re: Lumber Liquidators Chinese-Manufactured Flooring Products Mktg., Sales Practices and Products Liability Litig.*, 109 F. Supp. 3d at 1383 ("Centralization will . . . conserve the resources of the parties, their counsel and the judiciary.").

Centralizing these actions under Section 1407 will ensure streamlined resolution of this litigation to the overall benefit of the parties and the judiciary. *In re Amoxicillin Patent & Antitrust Litig.*, 449 F. Supp. 601, 603 (J.P.M.L. 1978) (granting transfer and consolidation of

three cases "[b]ecause of the presence of complex factual questions and the strong likelihood that discovery concerning these questions will be both complicated and time-consuming, we rule that transfer under Section 1407 is appropriate at the present time even though only three actions are presently involved").

Accordingly, transfer to a single district court is appropriate for the just and efficient resolution of these cases.

C. The Southern District of New York Is an Appropriate and Optimal Transferree Forum, and Judge Roman Is an Appropriate Transferee Judge

Plaintiffs respectfully submit that the Southern District of New York is the superior forum for the centralized action, and Judge Roman the ideal transferee judge. In choosing an appropriate transferee forum, this Panel considers: (1) where the largest number of cases is pending; (2) where discovery has occurred; (3) where cases have progressed furthest; (4) the site of the occurrence of the common facts; (5) where the cost and inconvenience will be minimized; and (6) the experience, skill, and caseloads of available judges. *Manual for Complex Litigation*, § 20.132 (4th ed. 2004). While several of these criteria are not yet implicated due to the infancy of the Actions, the Judge Roman, in the Southern District of New York, presents the most appropriate forum for the transfer and centralization of these actions, primarily because it has a judiciary well experienced, is where two of the three currently pending Actions were filed, and is where Defendants AMCA and Quest are headquartered.

The first factor favors the Southern District of New York, given that two of the three current actions are pending there. The second and third factors are not relevant here because discovery has not yet occurred in any case, and none of the Defendants have answered the Complaints or otherwise appeared.

As to the fourth factor, Defendant AMCA is a New York corporation with its principal place of business in Elmsford, New York. The Data Breach at issue occurred after an unauthorized user gained access to AMCA's system that contained information that AMCA had received from various entities. AMCA was the first of the Defendants to learn of the Data Breach and, thus, AMCA was first of the Defendants to breach its duty to disclose the Data Breach. While the relevant services are provided throughout the United States, so no one specific location is the dominant site of all common facts, the fact that the Data Breach occurred through AMCA's system argues forcefully for New York being the dominant site of the most relevant occurrence.

In addition, Defendant Quest, which first disclosed the Data Breach through an SEC filing, is headquartered in the Southern District of New York. As that filing disclosed, the Data Breach compromised some 11.9 million of Quest's patients' records.

The fifth factor favors the Southern District of New York given that AMCA and Quest are headquartered there, and that District likely is where the most important witnesses and evidence will be located.

The sixth factor favors Judge Roman, who is an experienced and capable judge, and was assigned to the earliest filed case in the Southern District of New York, the *Worthey* action. Judge Karas, who presides over the *Guttierez* action, already presides over one MDL, *IN RE: Ford Fusion and C-Max Fuel Economy Litigation*, MDL No. 2450. Otherwise, this factor is neutral as between the Central District of California and the Southern District of New York, given that both Districts have many experienced judges capable of handling a complex MDL actions such as this, both Districts regularly manage such actions, and both currently have a significant number of such actions pending.

When considered together, these factors support transfer and centralization in the Southern District of New York.

III. CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that her motion be granted and that the Panel order transfer of the Actions listed in the attached Schedule of Actions, plus any future tag-along actions, to the Southern District of New York, before Judge Nelson S. Roman, for consolidated pretrial proceedings in accordance with 28 U.S.C. § 1407.

Respectfully submitted,

Dated: June 4, 2019

AHDOOT & WOLFSON, PC

/s/ Tina Wolfson
Tina Wolfson
twolfson@ahdootwolfson.com
Brad King
bking@ahdootwolfson.com
Theodore W. Maya
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
45 Main Street, Suite 528
Brooklyn, NY 11201
Tel: 917-336-0171
Fax: 917-336-0177

Russell Yankwitt
russell@yankwitt.com
Michael H. Reed
michael@yankwitt.com
YANKWITT LLP
140 Grand Street
Suite 705
White Plains, NY 10601
Tel: 914-686-1500
Fax: 914-487-5000

Counsel for Plaintiff

and the Putative Classes

BEFORE THE UNITED STATES JUDICIAL PANEL ON
MULTI-DISTRICT LITIGATION

In re: American Medical Collection Agency Data Breach Litigation	MDL No.

SCHEDULE OF ACTIONS

#	Case Caption	Court	Civil Action No.	Judge
1	**Plaintiff:** Paula Worthey **Defendants:** Defendants American Medical Collection Agency, Inc.; Optum360 Services, Inc.; and Quest Diagnostics Incorporated	U.S. District Court, Southern District of New York	7:19-cv-05210	Hon. Nelson S. Roman
2	**Plaintiff:** Edgar Gutierrez **Defendants:** Defendants American Medical Collection Agency, Inc.; Optum360 Services, Inc.; and Quest Diagnostics Incorporated	U.S. District Court, Southern District of New York	7:19-cv-05212	Hon. Kenneth M. Karas
3	**Plaintiff:** Misty Marler **Defendants:** Defendants American Medical Collection Agency, Inc.; Optum360 Services, Inc.; and Quest Diagnostics Incorporated	U.S. District Court, Central District of California	8:19-cv-01091	TBD

Respectfully submitted,

Dated: June 4, 2019

AHDOOT & WOLFSON, PC

/s/ Tina Wolfson

Tina Wolfson
twolfson@ahdootwolfson.com
Brad King
bking@ahdootwolfson.com
Theodore W. Maya
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
45 Main Street, Suite 528
Brooklyn, NY 11201
Tel: 917-336-0171
Fax: 917-336-0177

Russell Yankwitt
russell@yankwitt.com
Michael H. Reed
michael@yankwitt.com
YANKWITT LLP
140 Grand Street
Suite 705
White Plains, NY 10601
Tel: 914-686-1500
Fax: 914-487-5000

Counsel for Plaintiff
and the Putative Classes

BEFORE THE UNITED STATES JUDICIAL PANEL ON
MULTI-DISTRICT LITIGATION

In re: American Medical Collection Agency Data Breach Litigation	MDL No.

CERTIFICATE OF SERVICE

I, Tina Wolfson, counsel for Plaintiff Paula Worthey hereby certify that on June 4, 2019, I caused to be filed a MOTION OF PLAINTIFF PAULA WORTHEY FOR TRANSFER AND CENTRALIZATION PURSUANT TO 28 U.S.C. § 1407 electronically using the Court's electronic case filing (CM/ECF) system, which automatically generated and sent a notice of electronic filing to the following e-mail addresses of all counsel of record, and served via U.S. mail on the following parties that have not yet appeared (as indicated):

Counsel and Defendants in *Worthey v. American Medical Collection Agency, Inc. et al.*:

Attorneys for Plaintiff Paula Worthey:

Russell Yankwitt
YANKWITT LLP
140 Grand Street
Suite 705
White Plains, NY 10601
Tel: 914-686-1500
Fax: 914-487-5000

Tina Wolfson
AHDOOT & WOLFSON, PC
45 Main Street, Suite 528
Brooklyn, NY 11201
Tel: 917-336-0171
Fax: 917-336-0177

Defendant American Medical Collection Agency, Inc.:

4 Westchester Plaza # 110
Elmsford, NY 10523

Defendant Optum360 Services, Inc.:

11000 Optum Circle
Eden Prairie, MN 55344

Defendant Quest Diagnostics Incorporated:

S500 Plaza Dr.
Secaucus, NJ 07094

Counsel and Defendants in *Gutierrez v. Am. Medical Collection Agency, Inc., et al.*:

Attorneys for Plaintiff Edgar Gutierrez:

Jeremiah Frei-Pearson
FINKELSTEIN, BLANKINSHIP,
FREI-PEARSON & GARBER, LLP
445 Hamilton A venue, Suite 605
White Plains, NY 1060

Defendant American Medical Collection Agency, Inc.:

4 Westchester Plaza # 110
Elmsford, NY 10523

Defendant Optum360 Services, Inc.:

11000 Optum Circle
Eden Prairie, MN 55344

Defendant Quest Diagnostics Incorporated:

S500 Plaza Dr.
Secaucus, NJ 07094

Counsel and Defendants in *Marler v. Quest Diagnostics, Inc., et al.*:

Attorneys for Plaintiff Misty Marler:

Daniel S. Robinson
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Dr.
Newport Beach, CA 92660

Defendant American Medical Collection Agency, Inc.:

4 Westchester Plaza # 110
Elmsford, NY 10523

Defendant Optum360 Services, Inc.:

11000 Optum Circle
Eden Prairie, MN 55344

Defendant Quest Diagnostics Incorporated:

S500 Plaza Dr.
Secaucus, NJ 07094

Respectfully submitted,

Dated: June 4, 2019

AHDOOT & WOLFSON, PC

/s/ Tina Wolfson

Tina Wolfson
twolfson@ahdootwolfson.com
Brad King
bking@ahdootwolfson.com
Theodore W. Maya
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
45 Main Street, Suite 528
Brooklyn, NY 11201
Tel: 917-336-0171
Fax: 917-336-0177

Russell Yankwitt
russell@yankwitt.com
Michael H. Reed
michael@yankwitt.com
YANKWITT LLP
140 Grand Street
Suite 705
White Plains, NY 10601
Tel: 914-686-1500
Fax: 914-487-5000

Counsel for Plaintiff
and the Putative Classes

ECF

U.S. District Court
Southern District of New York (White Plains)
CIVIL DOCKET FOR CASE #: 7:19-cv-05210-NSR

Worthey v. American Medical Collection Agency, Inc. et al
Assigned to: Judge Nelson Stephen Roman
Demand: $5,000,000
Cause: 28:1332ct Diversity-(Citizenship)

Date Filed: 06/03/2019
Jury Demand: Plaintiff
Nature of Suit: 190 Contract: Other
Jurisdiction: Diversity

Plaintiff

Paula Worthey
individually and on behalf of all others similarly situated

represented by **Russell Marc Yankwitt**
Yankwitt LLP
140 Grand Street, Suite 705
White Plains, NY 10601
(914)-686-1500
Fax: (914)-801-5930
Email: russell@yankwitt.com
ATTORNEY TO BE NOTICED

V.

Defendant

American Medical Collection Agency, Inc.

Defendant

Optum360 Services, Inc.

Defendant

Quest Diagnostics Incorporated

Defendant

DOES 1-10

Date Filed	#	Docket Text
06/03/2019	1	**FILING ERROR - DEFICIENT PLEADING - SIGNATURE ERROR -** COMPLAINT against American Medical Collection Agency, Inc., DOES 1-10, Optum360 Services, Inc., Quest Diagnostics Incorporated. (Filing Fee $ 400.00, Receipt Number ANYSDC-17010988)Document filed by Paula Worthey.(Yankwitt, Russell) Modified on 6/4/2019 (sj). (Entered: 06/03/2019)

06/03/2019	2	CIVIL COVER SHEET filed. (Yankwitt, Russell) (Entered: 06/03/2019)
06/03/2019	3	REQUEST FOR ISSUANCE OF SUMMONS as to AMERICAN MEDICAL COLLECTION AGENCY, INC., OPTUM360 SERVICES, INC., and QUEST DIAGNOSTICS INCORPORATED, re: 1 Complaint. Document filed by Paula Worthey. (Yankwitt, Russell) (Entered: 06/03/2019)
06/04/2019		*****NOTICE TO ATTORNEY REGARDING DEFICIENT PLEADING. Notice to Attorney Russell Marc Yankwitt to RE-FILE Document No. 1 Complaint. The filing is deficient for the following reason(s): the pleading was not signed. Re-file the pleading using the event type Complaint found under the event list Complaints and Other Initiating Documents - attach the correct signed PDF - select the individually named filer/filers - select the individually named party/parties the pleading is against. (sj)** (Entered: 06/04/2019)
06/04/2019		*****NOTICE TO ATTORNEY REGARDING CIVIL. CASE OPENING STATISTICAL ERROR CORRECTION: Notice to attorney Russell Marc Yankwitt. The following case opening statistical information was erroneously selected/entered: County code Westchester. The following correction(s) have been made to your case entry: the County code has been modified to XX Out of State. (sj)** (Entered: 06/04/2019)
06/04/2019		CASE OPENING INITIAL ASSIGNMENT NOTICE: The above-entitled action is assigned to Judge Nelson Stephen Roman. Please download and review the Individual Practices of the assigned District Judge, located at http://nysd.uscourts.gov/judges/District. Attorneys are responsible for providing courtesy copies to judges where their Individual Practices require such. Please download and review the ECF Rules and Instructions, located at http://nysd.uscourts.gov/ecf_filing.php. (sj) (Entered: 06/04/2019)
06/04/2019		Magistrate Judge Paul E. Davison is so designated. Pursuant to 28 U.S.C. Section 636(c) and Fed. R. Civ. P. 73(b)(1) parties are notified that they may consent to proceed before a United States Magistrate Judge. Parties who wish to consent may access the necessary form at the following link: http://nysd.uscourts.gov/forms.php. (sj) (Entered: 06/04/2019)
06/04/2019		Case Designated ECF. (sj) (Entered: 06/04/2019)
06/04/2019	4	ELECTRONIC SUMMONS ISSUED as to American Medical Collection Agency, Inc., Optum360 Services, Inc., Quest Diagnostics Incorporated. (sj) (Entered: 06/04/2019)
06/04/2019	5	COMPLAINT against American Medical Collection Agency, Inc., DOES 1-10, Optum360 Services, Inc., Quest Diagnostics Incorporated. Document filed by Paula Worthey.(Yankwitt, Russell) (Entered: 06/04/2019)

PACER Service Center			
Transaction Receipt			
06/04/2019 17:56:38			
PACER Login:	tmaya223242	**Client Code:**	AMCA

Description:	Docket Report	**Search Criteria:**	7:19-cv-05210-NSR
Billable Pages:	2	**Cost:**	0.20

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

PAULA WORTHEY, individually and on behalf of all others similarly situated,

Plaintiff,

v.

AMERICAN MEDICAL COLLECTION AGENCY, INC., OPTUM360 SERVICES, INC., QUEST DIAGNOSTICS INCORPORATED, and DOES 1-10,

Defendants.

Case No. 7:19-cv-5210

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiff Paula Worthey, on behalf of herself and all others similarly situated, through the undersigned counsel, hereby alleges the following, against Defendants American Medical Collection Agency, Inc. ("AMCA"), Optum360 Services, Inc. ("Optum360"), and Quest Diagnostics Incorporated ("Quest") (collectively, "Defendants"), upon her own knowledge or, where she lacks personal knowledge, upon information and belief including the investigation of her counsel, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action on behalf of a nationwide class and a California Sub-Class (together, the "Classes") against Defendants because of their failure to protect the confidential information of millions of patients—including financial information (e.g., credit card numbers and bank account information), medical information, personal information (e.g., Social Security Numbers), and/or other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Sensitive Information"). Defendants' wrongful disclosure has harmed Plaintiff.

II. PARTIES

2. Plaintiff Paula Worthey is an individual residing in Ventura, California, who has been a patient of Quest and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

3. Defendant American Medical Collection Agency, Inc. ("AMCA") is a New York corporation with its principal place of business in Elmsford, New York.

4. Defendant Quest Diagnostics Incorporated ("Quest") is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

5. Based on information and belief, Defendant Optum360 Services, Inc. ("Optum360") is a Delaware corporation with its principal place of business in Eden Praire Minnesota.

III. JURISDICTION AND VENUE

6. Subject Matter Jurisdiction. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiff is a citizen of California (and the proposed class members are from various states) while Defendants are citizens of the States of New York, Delaware, and New Jersey; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

7. Personal Jurisdiction. This Court has personal jurisdiction over Defendants because Defendants do business in and throughout the State of New York, and the wrongful acts alleged in this Complaint were committed in New York, among other venues.

8. Venue. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to the claims occurred in Westchester County, New York; and (2) 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

IV. FACTUAL ALLEGATIONS

9. Quest is the world's leading provider of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

10. On June 3, 2019, Quest publicly admitted in a filing with the Securities and Exchange Commission ("SEC") that: "On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest . . . and Optum360 LLC, [Quest's] revenue cycle management provider," of a massive data breach compromising the Sensitive Information of 11.9 million Quest patients, and most likely others (the "Data Breach"). Quest Form 8-K, June 3, 2019.

11. Quest's SEC filing disclosed that, "between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself[,] . . . include[ing] financial information (e.g., credit card numbers and bank account information), medical information[,] and other personal information (e.g., Social Security Numbers)." *Id.*

12. Quest apparently allowed hackers to access Plaintiff's and other Class Members' Sensitive Information for some seven months, and did nothing to let the victims know about the Data Breach for nearly a year after it began.

13. Although Quest knew of the Data Breach at least as of May 14, 2019, and although AMCA knew of it even earlier, neither took any steps to notify patients whose information was affected until June 3, 2019, at which point Quest only did so through an SEC filing.

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

15. Indeed, Quest promises patients that it will keep their Sensitive Information confidential, assuring patients that it is "committed to protecting the privacy of your identifiable health information." <http://questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html> (last visited June 3, 2019).

16. In its Notice of Privacy Practices, Quest acknowledges that it is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). *Id*.

17. Quest informs patients: "We may provide your PHI [(Private Health Information)] to other companies or individuals that need the information to provide services to us. These other entities, known as 'business associates,' are required to maintain the privacy and security of PHI." *Id.*

18. Defendants' data security obligations and promises were particularly important given the substantial increase in data breaches — particularly those in the healthcare industry — preceding August 2018, which were widely known to the public and to anyone in Defendants' industries.

19. 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 Plaintiff's 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);

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

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

It is Well Established That Data Breaches Lead to Identity Theft

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

21. 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.[1] As the GAO Report states, this type of identity theft is the most

[1] *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

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.

22. 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."[2]

23. 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.

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

> "[L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[3]

25. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a 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.[4]

Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited June 3, 2019).

[2] *Id.* at 2, 9.

[3] *Id.* at 29 (emphasis added).

[4] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at*

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

27. 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.[5] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

28. Medical databases are especially valuable 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."[6] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

V. CLASS ACTION ALLEGATIONS

29. Class Definition. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Nationwide Class, and a California Sub-Class, defined as follows:

> Nationwide Class: All persons in the United States whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the breach announced by Quest on or around June 3, 2019.

---

https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 28, 2019).

[5] *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 3, 2019).

[6] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 3, 2019).

> California Sub-Class: All persons in the State of California whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the breach announced by Quest on or around June 3, 2019.

Excluded from the above Classes are Defendants, any entity in which Defendants have a controlling interest or that have a controlling interest in Defendants, and Defendants' legal representatives, assignees, and successors. Also excluded are the Judge to whom this case is assigned and any member of the Judge's immediate family.

30. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

31. Commonality. There are numerous questions of law and fact common to Plaintiff and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants' data security systems prior to the Data Breach met the requirements of laws including, for instance, HIPAA;

b. Whether Defendants' data security systems prior to the Data Breach met industry standards;

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

d. Whether Plaintiff's and other Class members are entitled to damages as a result of Defendants' conduct.

32. Typicality. Plaintiff's claims are typical of the claims of the Classes' claims. Plaintiff suffered the same injury as Class Members—*i.e.*, upon information and belief Plaintiff's Sensitive Information was compromised in the Data Breach.

33. Adequacy. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor her counsel have interests that are contrary to or that conflict with those of the proposed Classes.

34. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and other Class Members. The common issues arising from this conduct that affect Plaintiff and Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

35. Superiority. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions is low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendants. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendants' records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiff's claims

as well as the claims of other Class Members. Finally, proceeding as a class action provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

36. Injunctive and Declaratory Relief Appropriate. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

FIRST CLAIM FOR RELIEF

Negligence

(On behalf of Plaintiff and the Nationwide Class)

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

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

39. 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.

40. 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.

41. Defendants also owed a duty of care to Plaintiff 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.

42. Defendants' duty to use reasonable security measures arose as a 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 Plaintiff and the members of the Classes from a data breach.

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

44. 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.

45. 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.

46. 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.

47. 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 Plaintiff's and Class members' Sensitive Information;

b. failing to adequately monitor the security of AMCA's networks and systems;

c. allowing unauthorized access to Plaintiff's and Class members' Sensitive Information;

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

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

48. 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 Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Classes were reasonably foreseeable.

49. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff 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.

50. Accordingly, Plaintiff, on behalf of herself and members of the Classes seek an order declaring that Defendants' conduct constitutes negligence, and awarding damages in an amount to be determined at trial.

SECOND CLAIM FOR RELIEF

Violation of the California Confidential Medical Information Act

(On behalf of Plaintiff and the California Sub-Class)

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

52. Plaintiff alleges additionally and alternatively that California's Confidential Medical Information Act was enacted to protect, among other things, the release of confidential medical information without proper authorization. *See* Confidential Medical Information Act, Cal. Civ. Code §§ 56, *et seq.* ("CMIA"). To that end, the CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information. *See* Cal. Civ. Code § 56.36 (2013). The CMIA also requires that an entity that "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Civ. Code § 56.101(a).

53. As described throughout this Complaint, Defendants negligently disclosed and released Plaintiff's and California Sub-Class Members' Sensitive Information by failing to implement adequate security protocols to prevent unauthorized access to Sensitive Information, failing to maintain an adequate electronic security system to prevent data breaches, failing to employ industry standard and commercially viable measures to mitigate the risks of any data breach, and otherwise failing to comply with HIPAA data security requirements.

54. As a direct and proximate result of Defendants' negligence, they disclosed and released Plaintiff's and California Sub-Class Members' Sensitive Information to hackers.

55. Accordingly, Plaintiff seeks to recover actual, nominal (including $1000 nominal damages per disclosure under Cal. Civ. Code § 56.36(b)), and statutory damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

THIRD CLAIM FOR RELIEF

Violation of New York General Business Law § 349

(On behalf of Plaintiff and the Nationwide Class)

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

57. 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).

58. 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.

59. 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.

60. 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-named unfair practices and deceptive acts were negligent, knowing and willful.

61. Plaintiff seeks 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. *Id.*

62. 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.

63. 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.

FOURTH CLAIM FOR RELIEF

Breach of Implied Contract (On Behalf of Plaintiff and the Nationwide Class)

64. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

65. Plaintiff brings this cause of action on behalf of the Class and to the extent necessary.

66. When Plaintiff and Class members paid money and provided their Sensitive Information 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.

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

68. Plaintiff and the Class would not have provided and entrusted their Sensitive Information to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

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

70. Defendants breached their implied contracts with Plaintiff and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

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

FIFTH CLAIM FOR RELIEF

Violation of the California Unfair Competition Act, Cal. Bus. & Prof. Code § 17200, *et seq.*

(On behalf of Plaintiff and the California Sub-Class)

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

73. Defendants' actions as described herein constitute unfair competition within the meaning of the UCL, insofar as the UCL prohibits "any unlawful, unfair or fraudulent business act or practice."

74. Defendants' conducts as alleged herein constitute unlawful, unfair, and fraudulent business practices in that they deceived the Plaintiff and California Sub-Class Members into believing their Sensitive Information would be protected by reasonable, industry-standard data security measures.

75. Defendants' conduct constitutes an "unlawful" business practice within the meaning of the UCL because it violates HIPAA, the California Customer Records Act, Cal. Civ. Code § 17980.80 *et seq.*, and other statutes requiring adequate data security to protect Sensitive Information such as that which was compromised in the Data Breach.

76. Defendants' conduct constitutes an "unfair" business practice within the meaning of the UCL because it is immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers.

77. As a direct and proximate result of Defendants' wrongful business practices in violation of the UCL, the California Plaintiff and California Sub-Class Members have suffered injury in fact and lost money or property as a result of purchasing services from Quest. The California Plaintiff and California Sub-Class Members would not have purchased or paid as much for services from Quest had they known the truth about Defendants' data security.

78. Defendants' wrongful business practices constitute a continuing course of conduct of unfair competition since Defendants continues to employ deficient data security.

79. Pursuant to Cal. Bus. & Prof. Code § 17203, the California Plaintiff and the California Sub-Class Members seek an order of this Court enjoining Defendants from continuing to engage in unlawful, unfair, and fraudulent business practices and any other act prohibited by law, including those set forth in this Complaint. The California Plaintiff and the California Sub-Class Members also seek an order requiring Defendants to make full restitution of all moneys it wrongfully obtained from the California Plaintiffs and the Class.

80. Pursuant to Cal. Bus. & Prof. Code § 17203, the California Plaintiff and California Sub-Class Members seek an injunction enjoining Defendant from continuing to employ deficient data security.

SIXTH CLAIM FOR RELIEF

Violation of the California's Customer Records Act, Cal. Civil Code §§ 1798.81.5 & 1798.82

(On behalf of Plaintiff and the California Sub-Class)

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

82. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code section 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

83. The Sensitive Information taken in the Data Breach fits within the definition of "Personal information" in Civil Code section 1798.80.

84. Plaintiff and other Class Members provided their personal information to Defendants in order to get medical diagnoses. These patients qualify as "Customer[s]" as defined in Civil Code section 1798.80.

85. By failing to implement reasonable measures to protect the Sensitive Information in their possession, Defendants violated Civil Code section 1798.81.5.

86. In addition, by failing to promptly notify all who were affected by the Data Breach that their Sensitive Information had been acquired (or was reasonably believed to have been acquired) by hackers, Defendants violated Civil Code Section 1798.82.

87. As a direct or proximate result of Defendants' violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Plaintiff and Class Members were (and continue to be) injured

and have suffered (and will continue to suffer) the damages described in this Class Action Complaint.

88. Defendants' violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82 were, at a minimum, reckless.

89. In addition, by violating Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Defendants "may be enjoined" under Civil Code Section 1798.84(e).

90. Defendants' violations of Civil Code Section 1798.81.5 and 1798.82 also constitute an unlawful acts or practices under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 *et seq.*, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

91. Plaintiff accordingly requests that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendants utilize strong industry standard encryption algorithms for encryption keys that provide access to stored Sensitive Information; (2) ordering that Defendants implement the use of encryption keys in accordance with industry standards; (3) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on systems belong to Defendants and all others with whom they share Sensitive Information, on a periodic basis; (4) ordering that Defendants engage third-party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendants audit, test and train their security personnel regarding any new or modified procedures; (6) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' computer system is compromised, hackers cannot gain access to other portions of their systems; (7) ordering that Defendants purge, delete, destroy in a reasonable secure manner Sensitive Information no longer

necessary; (8); ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering that Defendants implement industry best practices data security systems..

92. Plaintiff further requests that the Court require Defendants to identify and notify all members of the nationwide Class who have not yet been informed of the Data Breach.

93. Plaintiff and the Class are entitled to actual damages in an amount to be determined at trial under Civil Code Section 1798.84.

94. Plaintiff and the Class also are entitled to an aware of attorney fees and costs under Civil Code Section 1798.84.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on her own behalf and on behalf of Class Members, pray for judgment against Defendant as follows:

A. Certification of the proposed Classes;

B. Appointment of Plaintiff as Class representative;

C. Appointment of the undersigned counsel as counsel for the Classes;

D. Declaring that Defendants' actions, as described above, constitute negligence and amounted to violations of HIPAA, the California Customer Records Act, the California Confidential Medical Information Act, and the consumer protection laws of New York, California, and other states;

H. An award to Plaintiff and the Classes of damages, as allowed by law;

I. An award to Plaintiff and the Classes of attorneys' fees and costs, as allowed by law and/or equity;

J. Leave to amend this Complaint to conform to the evidence presented at trial; and

K. Orders granting such other and further relief as the Court deems necessary, just, and proper.

VII. DEMAND FOR JURY

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

Dated: June 3, 2019

YANKWITT LLP

Russell Yankwitt
russell@yankwitt.com
Michael H. Reed
michael@yankwitt.com
140 Grand Street
Suite 705
White Plains, NY 10601
Tel: 914-686-1500
Fax: 914-487-5000

Tina Wolfson (NY Bar No. 5436043)
twolfson@ahdootwolfson.com
Brad King (NY Bar No. 5588336)
bkink@ahdootwolfson.com
Theodore W. Maya (*pro hac vice* pending)
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
45 Main Street, Suite 528
Brooklyn, NY 11201
Tel: 917-336-0171
Fax: 917-336-0177

Counsel for Plaintiff
and the Putative Classes

ECF

U.S. District Court
Southern District of New York (White Plains)
CIVIL DOCKET FOR CASE #: 7:19-cv-05212-KMK

Gutierrez v. American Medical Collection Agency, Inc. et al
Assigned to: Judge Kenneth M. Karas
Demand: $5,000,000
Cause: 28:1332 Diversity Action

Date Filed: 06/03/2019
Jury Demand: Plaintiff
Nature of Suit: 190 Contract: Other
Jurisdiction: Diversity

Plaintiff

Edgar Gutierrez
individually and on behalf of all others similarly situated

represented by **Jeremiah Lee Frei-Pearson**
Finkelstein Blankinship, Frei-Pearson & Garber, LLP
445 Hamilton Ave, Suite 605
White Plains, NY 10601
914-298-3281
Fax: 914-824-1561
Email: jfrei-pearson@fbfglaw.com
ATTORNEY TO BE NOTICED

V.

Defendant

Quest Diagnostics Incorporated

Defendant

American Medical Collection Agency, Inc.

Defendant

Optum360, LLC

Defendant

Does 1-10

Date Filed	#	Docket Text
06/03/2019	1	COMPLAINT against American Medical Collection Agency, Inc., Does 1-10, Optum360, LLC, Quest Diagnostics Incorporated. (Filing Fee $ 400.00, Receipt Number ANYSDC-17011099)Document filed by Edgar Gutierrez.(Frei-Pearson, Jeremiah) (Entered: 06/03/2019)

06/03/2019	2	CIVIL COVER SHEET filed. (Frei-Pearson, Jeremiah) (Entered: 06/03/2019)
06/03/2019	3	REQUEST FOR ISSUANCE OF SUMMONS as to AMERICAN MEDICAL COLLECTION AGENCY, INC., re: 1 Complaint. Document filed by Edgar Gutierrez. (Frei-Pearson, Jeremiah) (Entered: 06/03/2019)
06/03/2019	4	REQUEST FOR ISSUANCE OF SUMMONS as to QUEST DIAGNOSTICS INCORPORATED, re: 1 Complaint. Document filed by Edgar Gutierrez. (Frei-Pearson, Jeremiah) (Entered: 06/03/2019)
06/03/2019	5	REQUEST FOR ISSUANCE OF SUMMONS as to OPTUM360, LLC, re: 1 Complaint. Document filed by Edgar Gutierrez. (Frei-Pearson, Jeremiah) (Entered: 06/03/2019)
06/04/2019		*****NOTICE TO ATTORNEY REGARDING PARTY MODIFICATION. Notice to attorney Jeremiah Lee Frei-Pearson. The party information for the following party/parties has been modified: Edgar Gutierrez. The information for the party/parties has been modified for the following reason/reasons: party text was omitted. (sj)** (Entered: 06/04/2019)
06/04/2019		*****NOTICE TO ATTORNEY REGARDING CIVIL. CASE OPENING STATISTICAL ERROR CORRECTION: Notice to attorney Jeremiah Lee Frei-Pearson. The following case opening statistical information was erroneously selected/entered: County code Albany. The following correction(s) have been made to your case entry: the County code has been modified to XX Out of State. (sj)** (Entered: 06/04/2019)
06/04/2019		CASE OPENING INITIAL ASSIGNMENT NOTICE: The above-entitled action is assigned to Judge Kenneth M. Karas. Please download and review the Individual Practices of the assigned District Judge, located at http://nysd.uscourts.gov/judges/District. Attorneys are responsible for providing courtesy copies to judges where their Individual Practices require such. Please download and review the ECF Rules and Instructions, located at http://nysd.uscourts.gov/ecf_filing.php. (sj) (Entered: 06/04/2019)
06/04/2019		Magistrate Judge Judith C. McCarthy is so designated. Pursuant to 28 U.S.C. Section 636(c) and Fed. R. Civ. P. 73(b)(1) parties are notified that they may consent to proceed before a United States Magistrate Judge. Parties who wish to consent may access the necessary form at the following link: http://nysd.uscourts.gov/forms.php. (sj) (Entered: 06/04/2019)
06/04/2019		Case Designated ECF. (sj) (Entered: 06/04/2019)
06/04/2019	6	ELECTRONIC SUMMONS ISSUED as to American Medical Collection Agency, Inc.. (sj) (Entered: 06/04/2019)
06/04/2019	7	ELECTRONIC SUMMONS ISSUED as to Quest Diagnostics Incorporated. (sj) (Entered: 06/04/2019)
06/04/2019	8	ELECTRONIC SUMMONS ISSUED as to Optum360, LLC. (sj) (Entered: 06/04/2019)

PACER Service Center

Transaction Receipt

06/04/2019 17:02:19

PACER Login:	tmaya223242	**Client Code:**	AMCA
Description:	Docket Report	**Search Criteria:**	7:19-cv-05212-KMK
Billable Pages:	2	**Cost:**	0.20

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

EDGAR GUTIERREZ, individually and on behalf of all others similarly situated,

Plaintiff,

v.

AMERICAN MEDICAL COLLECTION AGENCY, INC., OPTUM360, LLC, QUEST DIAGNOSTICS INCORPORATED, and DOES 1-10,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiff Edgar Gutierrez, on behalf of himself and all others similarly situated, through the undersigned counsel, hereby alleges the following, against Defendants American Medical Collection Agency, Inc. ("AMCA"), Optum360, LLC ("Optum360"), and Quest Diagnostics Incorporated ("Quest") (collectively, "Defendants"), upon his own knowledge or, where he lacks personal knowledge, upon information and belief including the investigation of his counsel as follows:

I. INTRODUCTION

1. Plaintiff, on behalf of a nationwide class and a California Sub-Class (together, the "Classes"), brings this class action lawsuit against Defendants because Defendants unlawfully disclosed the confidential information of millions of patients—including financial information (e.g., credit card numbers and bank account information), medical information, and other personal information (e.g., Social Security Numbers), and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Sensitive Information"). Defendants' wrongful disclosure has harmed Plaintiffs

II. PARTIES

2. Plaintiff Edgar Gutierrez is an individual residing in Oxnard, California, who has been a patient of Quest and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

3. Defendant American Medical Collection Agency, Inc. ("AMCA") is a New York corporation with its principal place of business in Elmsford, New York.

4. Defendant Quest Diagnostics Incorporated is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

5. Based on information and belief, Defendant Optum360, LLC. is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota.

III. JURISDICTION AND VENUE

6. Subject Matter Jurisdiction. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) Plaintiff proposes a nationwide class action, while Defendants are citizens of the States of New York, New Jersey, and Delaware; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

7. Personal Jurisdiction. This Court has personal jurisdiction over Defendants because Defendants do business in and throughout the State of New York, and the wrongful acts alleged in this Complaint were committed in New York, among other venues.

8. Venue. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to the claims occurred in Westchester County, New York; and (2) 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

IV. FACTUAL ALLEGATIONS

9. Quest is the world's leading provider of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

10. On June 3, 2019, Quest publicly admitted in a filing with the Securities and Exchange Commission ("SEC") that: "On May 14, 2019, American Medical Collection Agency

(AMCA), a billing collections vendor, notified Quest . . . and Optum360 LLC, [Quest's] revenue cycle management provider," of a massive data breach compromising the Sensitive Information of 11.9 million Quest patients, and most likely others (the "Data Breach"). Quest Form 8-K, June 3, 2019.

11. Quest's SEC filing disclosed that, "between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself[,] . . . include[ing] financial information (e.g., credit card numbers and bank account information), medical information[,] and other personal information (e.g., Social Security Numbers)." *Id.*

12. Quest apparently allowed hackers to have access to Plaintiff's and other Class Members' Sensitive Information for some seven months, and did nothing to let the victims know about the Data Breach for nearly a year after it began.

13. Although Quest knew of the Data Breach at least as of May 14, 2019, and although AMCA knew of it even earlier, neither took any steps to notify patients whose information was affected until June 3, at which point Quest only did so through an SEC filing.

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

15. Indeed, Quest promises patients that it will keep their Sensitive Information confidential, assuring patients that it is "committed to protecting the privacy of your identifiable

health information." <http://questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html> (last visited June 3, 2019).

16. In its Notice of Privacy Practices, Quest acknowledges that it is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). *Id.*

17. Quest informs patients: "We may provide your PHI to other companies or individuals that need the information to provide services to us. These other entities, known as 'business associates,' are required to maintain the privacy and security of [Private Health Information, known as] PHI." *Id.*

18. Defendants' data security obligations and promises were particularly important given the substantial increase in data breaches — particularly those in the healthcare industry — preceding August 2018, which were widely known to the public and to anyone in Defendants' industries.

19. 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 Plaintiff's and the Classes' Sensitive Information;

c. Ensuring the confidentiality and integrity of electronic protected health information they created, received, maintained, and/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);

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 workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

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

It is Well Established That Data Breaches Lead to Identity Theft

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

21. 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.[1] As the GAO Report states, this type of identity theft is the most

[1] *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 3, 2019).

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.

22. 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."[2]

23. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

24. There may be a time lag between when sensitive informationformation 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.[3]

25. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a 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, and 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.[4]

---

[2] *Id.* at 2, 9.
[3] *Id*. at 29 (emphasis added).
[4] *See* Federal Trade Commission, *Warning Signs of Identity Theft, available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 28, 2019).

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

27. 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.[5] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

28. 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."[6] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

V. CLASS ACTION ALLEGATIONS

29. Class Definition. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Nationwide Class, and a California Sub-Class, defined as follows:

> Nationwide Class: All persons in the United States whose Sensitive Information was maintained on AMCA's systems that were compromised as a result of the breach announced by Quest on or around June 3, 2019.

[5] *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 3, 2019).
[6] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 3, 2019).

> California Sub-Class: All persons in the State of California whose Sensitive Information was maintained on AMCA's systems that were compromised as a result of the breach announced by Quest on or around June 3, 2019.

Excluded from the above Classes are Defendants, any entity in which Defendants have a controlling interest or that have a controlling interest in Defendants, and Defendants' legal representatives, assignees, and successors. Also excluded are the Judge to whom this case is assigned and any member of the Judge's immediate family.

30. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

31. Commonality. There are numerous questions of law and fact common to Plaintiffs and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants' data security systems prior to the Data Breach met the requirements of laws including, for instance, HIPAA;

b. Whether Defendants' data security systems prior to the Data Breach met industry standards;

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

d. Whether Plaintiffs and other Class members are entitled to damages as a result of Defendants' conduct.

32. Typicality. Plaintiff's claims are typical of the claims of the Classes' claims. Plaintiff suffered the same injury as Class Members—*i.e.*, Plaintiff's Sensitive Information was compromised in the Data Breach.

33. Adequacy. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to or that conflict with those of the proposed Classes.

34. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and other Class Members. The common issues arising from this conduct that affect Plaintiff and Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

35. Superiority. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions is low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendants. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendants' records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiff's claims

as well as the claims of other Class Members. Finally, proceeding as a class action provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

36. Injunctive and Declaratory Relief Appropriate. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

FIRST CLAIM FOR RELIEF

Negligence

(On behalf of Plaintiff and the Nationwide Class)

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

38. Quest required Plaintiff and Class members to submit non-public Personal Information in order to obtain medical services, which it provided to AMCA for billing purposes.

39. 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. 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.

40. Defendants owed a duty of care to Plaintiff 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.

41. Defendants' duty of care to use reasonable security measures arose as a 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 Plaintiff and the members of the Classes from a data breach.

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

43. 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.

44. 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.

45. 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. 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 Plaintiff's and proposed members of the Classes' Sensitive Information;

b. failing to adequately monitor the security of AMCA's networks and systems;

c. allowing unauthorized access to Plaintiff's and the proposed members of the Classes' Sensitive Information;

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

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

46. 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 Plaintiff and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Classes were reasonably foreseeable.

47. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff 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.

48. Accordingly, Plaintiff, on behalf of himself and members of the Classes seek an order declaring that Defendants' conduct constitutes negligence, and awarding damages in an amount to be determined at trial.

SECOND CLAIM FOR RELIEF

Violation of the California Confidential Medical Information Act

(On behalf of Plaintiff and the California Sub-Class)

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

50. Plaintiff alleges additionally and alternatively that California's Confidential Medical Information Act was enacted to protect, among other things, the release of confidential medical information without proper authorization. *See* Confidential Medical Information Act, Cal. Civ. Code §§ 56, *et seq.* ("CMIA"). To that end, the CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information. *See* Cal. Civ. Code § 56.36 (2013). The CMIA also requires that an entity that "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Civ. Code § 56.101(a).

51. As described throughout this Complaint, Defendants negligently disclosed and released Plaintiffs' and California Sub-Class members' Sensitive Information by failing to implement adequate security protocols to prevent unauthorized access to Sensitive Information, failing to maintain an adequate electronic security system to prevent data breaches, failing to employ industry standard and commercially viable measures to mitigate the risks of any data breach, and otherwise failing to comply with HIPAA data security requirements.

52. As a direct and proximate result of Defendants' negligence, Defendants disclosed and released Plaintiffs' and California Sub-Class members' Sensitive Information to hackers.

53. Accordingly, Plaintiff seeks to recover actual, nominal (including $1000 nominal damages per disclosure under Cal. Civ. Code § 56.36(b)), and statutory damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

THIRD CLAIM FOR RELIEF

Violation of New York General Business Law § 349

(On behalf of Plaintiff and the Nationwide Class)

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

55. 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).

56. 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.

57. 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.

58. 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-named unfair practices and deceptive acts were negligent, knowing and willful.

59. Plaintiff seeks 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. *Id.*

60. 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.

61. 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.

FOURTH CLAIM FOR RELIEF

Breach of Implied Contract

(On Behalf of Plaintiff and the Nationwide Class)

62. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

63. Plaintiff brings this cause of action on behalf of the Class and to the extent necessary.

64. When Plaintiff and Class members paid money and provided their Sensitive Information 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.

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

66. Plaintiff and the Class would not have provided and entrusted their Sensitive Information to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

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

68. Defendants breached their implied contracts with Plaintiff and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

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

FIFTH CLAIM FOR RELIEF

Violation of the California Unfair Competition Act, Cal. Bus. & Prof. Code § 17200, *et seq.*

(On behalf of Plaintiff and the California Sub-Class)

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

71. Defendants' actions as described herein constitute unfair competition within the meaning of the UCL, insofar as the UCL prohibits "any unlawful, unfair or fraudulent business act or practice."

72. Defendants' conducts as alleged herein constitute unlawful, unfair, and fraudulent business practices in that they deceived the Plaintiff and California Sub-Class Members into believing their Sensitive Information would be protected by reasonable, industry-standard data security measures.

73. Defendant's conduct constitutes an "unlawful" business practice within the meaning of the UCL because it violates HIPAA, the California Customer Records Act, Cal. Civ. Code § 17980.80 *et seq.*, and other statutes requiring adequate data security to protect Sensitive Information such as that which was compromised in the Data Breach.

74. Defendant's conduct constitutes an "unfair" business practice within the meaning of the UCL because it is immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers.

75. As a direct and proximate result of Defendants' wrongful business practices in violation of the UCL, the California Plaintiff and California Sub-Class Members have suffered injury in fact and lost money or property as a result of purchasing services from Quest. Plaintiff and California Sub-Class Members would not have purchased or paid as much for services from Quest had they known the truth about Defendants' data security.

76. Defendant's wrongful business practices constitute a continuing course of conduct of unfair competition since Defendant continues to employ deficient data security.

77. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiff and the California Sub-Class Members seek an order of this Court enjoining Defendant from continuing to engage in unlawful, unfair, and fraudulent business practices and any other act prohibited by law, including those set forth in this Complaint. The California Plaintiff and the California Sub-Class Members also seek an order requiring Defendant to make full restitution of all moneys it wrongfully obtained from the California Plaintiffs and the Class.

Pursuant to Cal. Bus. & Prof. Code § 17203, the California Plaintiff and California Sub-Class Members seek an injunction enjoining Defendant from continuing to employ deficient data security.

SIXTH CLAIM FOR RELIEF

Violation of the California's Customer Records Act,

Cal. Civil Code §§ 1798.81.5 & 1798.82

(On behalf of Plaintiff and the California Sub-Class)

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

79. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code section 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

80. The Sensitive Information taken in the Data Breach fits within the definition of "Personal information" in Civil Code section 1798.80.

81. Plaintiff and other Class members provided their personal information to Defendants in order to get medical diagnoses. These patients qualify as "Customer[s]" as defined in Civil Code Section 1798.80.

82. By failing to implement reasonable measures to protect the Sensitive Information in their possession, Defendants violated Civil Code Section 1798.81.5.

83. In addition, by failing to promptly notify all who were affected by the Data Breach that their Sensitive Information had been acquired (or was reasonably believed to have been acquired) by hackers, Defendants violated Civil Code Section 1798.82.

84. As a direct or proximate result of Defendants' violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Plaintiff and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in this Class Action Complaint.

85. Defendants' violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82 were, at a minimum, reckless.

86. In addition, by violating Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Defendants "may be enjoined" under Civil Code Section 1798.84(e).

87. Defendants violations of Civil Code Section 1798.81.5 and 1798.82 also constitute an unlawful acts or practices under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 *et seq.*, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

88. Plaintiff accordingly request that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendants utilize strong industry standard encryption algorithms for encryption keys that provide access to stored Sensitive Information; (2) ordering that Defendants implement the use of encryption keys in accordance with industry standards; (3) ordering that Defendants, consistent with industry standard practices, engage third party security

auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on systems belong to Defendants and all others with whom they share Sensitive Information, on a periodic basis; (4) ordering that Defendants engage third-party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendants audit, test and train their security personnel regarding any new or modified procedures; (6) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' computer system is compromised, hackers cannot gain access to other portions of their systems; (7) ordering that Defendants purge, delete, destroy in a reasonable secure manner Sensitive Information no longer necessary; (8); ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering that Defendants implement industry best practices data security systems.

89. Plaintiffs further request that the Court require Defendants to identify and notify all members of the nationwide Class who have not yet been informed of the Data Breach.

90. Plaintiff and the Class are entitled to actual damages in an amount to be determined at trial under Civil Code Section 1798.84.

91. Plaintiff and the Class also are entitled to an aware of attorney fees and costs under Civil Code Section 1798.84.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on their own behalf and on behalf of Class Members, pray for judgment against Defendant as follows:

A. Certification of the proposed Classes;

B. Appointment of Plaintiff as a Class representatives;

C. Appointment of the undersigned counsel as counsel for the Classes;

D. Declaring that Defendants' actions, as described above, constitute negligence and amounted to violations of HIPAA, the California Customer Records Act, the California Confidential Medical Information Act, and the consumer protection laws of New York, California, and other states;

H. An award to Plaintiff and the Classes of damages, as allowed by law;

I. An award to Plaintiff and the Classes of attorneys' fees and costs, as allowed by law and/or equity;

J. Injunctive relief requiring as set forth in ¶ 88, *supra*;

K. Leave to amend this Complaint to conform to the evidence presented at trial; and

L. Orders granting such other and further relief as the Court deems necessary, just, and proper.

VII. DEMAND FOR JURY

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

Dated: June 3, 2019

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP

Jeremiah Frei-Pearson
D. Greg Blankinship
Todd S. Garber
Chantal Khalil
445 Hamilton Avenue, Suite 605
White Plains, NY 10601
Tel: 914-298-3281
jfrei-pearson@fbfglaw.com
gblankinship@fbfglaw.com
tgarber@fbfglaw.com
ckhalil@fbfglaw.com

Counsel for Plaintiff
and the Putative Classes

ACCO

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA (Southern Division - Santa Ana)
CIVIL DOCKET FOR CASE #: 8:19-cv-01091

Marler v. Quest Diagnostics, Inc. et al
Assigned to:
Cause: 28:1331 Fed. Question: Personal Injury

Date Filed: 06/03/2019
Jury Demand: Plaintiff
Nature of Suit: 360 P.I.: Other
Jurisdiction: Diversity

Plaintiff

Misty Marler

represented by **Daniel S Robinson**
Robinson Calcagnie Inc
19 Corporate Plaza Drive
Newport Beach, CA 92660
949-720-1288
Fax: 949-720-1292
Email: drobinson@robinsonfirm.com
ATTORNEY TO BE NOTICED

V.

Defendant

Quest Diagnostics, Inc.

Defendant

Optum360 Services, Inc.

Defendant

American Medical Collection Agency

Date Filed	#	Docket Text
06/03/2019	1	COMPLAINT Receipt No: 0973-23851653 - Fee: $400, filed by Plaintiff Misty Marler. (Attorney Daniel S Robinson added to party Misty Marler(pty:pla))(Robinson, Daniel) (Entered: 06/03/2019)
06/03/2019	2	CIVIL COVER SHEET filed by Plaintiff Misty Marler. (Robinson, Daniel) (Entered: 06/03/2019)
06/03/2019	3	NOTICE of Interested Parties filed by Plaintiff Misty Marler, identifying Quest Diagnostics, Inc., Optum360 Services, Inc., American Medical Collection Agency. (Robinson, Daniel) (Entered: 06/03/2019)

06/03/2019	4	First AMENDED COMPLAINT against Defendants American Medical Collection Agency, Optum360 Services, Inc., Quest Diagnostics, Inc. amending Complaint (Attorney Civil Case Opening) 1 , filed by Plaintiff Misty Marler(Robinson, Daniel) (Entered: 06/03/2019)
06/03/2019	5	Request for Clerk to Issue Subpoena filed by Plaintiff Misty Marler., Request for Clerk to Issue Summons on Amended Complaint/Petition 4 filed by Plaintiff Misty Marler. (Robinson, Daniel) (Entered: 06/03/2019)
06/03/2019	6	Request for Clerk to Issue Summons on Amended Complaint/Petition 4 filed by Plaintiff Misty Marler. (Robinson, Daniel) (Entered: 06/03/2019)
06/03/2019	7	Request for Clerk to Issue Summons on Amended Complaint/Petition 4 filed by Plaintiff Misty Marler. (Robinson, Daniel) (Entered: 06/03/2019)

PACER Service Center

Transaction Receipt

06/04/2019 14:58:15

PACER Login:	tmaya223242:4608217:0	**Client Code:**	AMCA
Description:	Docket Report	**Search Criteria:**	8:19-cv-01091 End date: 6/4/2019
Billable Pages:	1	**Cost:**	0.10

Daniel S. Robinson (SBN 244245)
Wesley K. Polischuk (SBN 254121)
Michael W. Olson (SBN 312857)
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288
Fax: (949) 720-1292
drobinson@robinsonfirm.com
wpolischuk@robinsonfirm.com
molson@robinsonfirm.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MISTY MARLER, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

QUEST DIAGNOSTICS, INC.; OPTUM360 SERVICES, INC.; AMERICAN MEDICAL COLLECTION AGENCY and DOES 1 through 100,

Defendants.

Case No.

FIRST AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Misty Marler ("Plaintiff"), individually, and on behalf of the class defined below, brings this class action complaint against Quest Diagnostics Inc. ("Quest Diagnostics"), American Medical Collection Agency ("AMCA"), Optum360 LLC ("Optum360"), and Does 1 through 100 ("Doe Defendants") (collectively, Quest Diagnostics, AMCA, Optum 360, and Doe Defendants are referred to as "Defendants") and alleges as follows:

INTRODUCTION

1. On June 3, 2019, Quest Diagnostics, one of the largest blood testing providers in the country, announced a data breach whereby nearly 12 million of its customers, including Plaintiff and putative Class members, had their personally identifiably information ("PII") and protected health information ("PHI") accessed by unauthorized parties due to the negligent data security of AMCA, one if its billing collections vendors (the "Data Breach"). Specifically, the PII and PHI accessed included, but was not limited to, Plaintiff's and Class members' personal information (e.g. Social Security Numbers), financial information (credit card numbers and bank account information), and medical information.

2. In its SEC filing relating to the Data Breach, Quest Diagnostics announced that unauthorized parties accessed between August 1, 2018 and March 30, 2019 AMCA's system, which contained Plaintiff's and Class members' PII and PHI.

3. Despite unauthorized parties having access to the AMCA system for more than six months, AMCA only learned of the Data Breach as a result of receiving information from a security compliance firm that works with credit card companies.

4. Given AMCA's relationship to Question Diagnostics (AMCA provides services to Optum360, which in turn provides payment services to Quest Diagnostics), Plaintiff and Class members were blindsided by the Data Breach announcement given most have never heard of AMCA or Optum360 and were unaware that their information would be shared with these entities, causing additional emotional harm.

5. Based on information and belief, AMCA informed Quest Diagnostics and

Optum360 of the Data Breach on May 14, 2019. Still, Quest Diagnostics and Optum360 waited more than two weeks to notify Plaintiff and Class members of the Data Breach.

6. Based on further information and belief, AMCA first learned of the Data Breach on or around March 30, 2019 but waited more than three months to notify Plaintiff and Class members of the Data Breach.

7. While nearly 12 million Data Breach victims sought out and/or paid for diagnostics testing and medical care from Defendants, thieves were hard at work, stealing and using their hard-to-change Social Security numbers and highly sensitive PII/PHI for nearly one year without the victims' knowledge. Defendants' lax security practices that allowed this intrusion to occur have worsened Plaintiff's and other Class members' lives by, among other injuries: (a) adding to their already heightened financial obligations by placing them at increased risk of fraudulent charges; (b) complicating diagnosis, prognosis, and treatment for their severe medical conditions by placing them at increased risk of having inaccurate medical information in their files; and/or (c) increasing the risk of other potential personal, professional, or financial harms that could be caused as a result of having their PII/PHI exposed.

8. Prior to the Data Breach, Quest Diagnostics acknowledged in its Notice of Privacy Practices that it is "committed to protecting the privacy of your identifiable health information" and that it would only use Plaintiff and Class members PII/PHI for certain limited purposes, such as for treatment, payment, or healthcare operations purposes and for other purposes permitted or required by law. Quest Diagnostics represented that it would abide by these obligations, but failed to live up to its own promises as well as its duties and obligations required by law and industry standards.

9. Contrary to its promises to help patients improve the quality of their lives through secure data practices, Defendants' conduct has instead been a direct cause of the ongoing harm to Plaintiffs and other Class members whose suffering has been magnified by the Data Breach, and who will continue to experience harm and data insecurity for the indefinite future.

10. Specifically, Defendants failed to maintain reasonable and/or adequate security measures to protect Plaintiff's and other Class members' PII/PHI from unauthorized access and disclosure, apparently lacking, at a minimum: (1) reasonable and adequate security measures designed to prevent this attack even though Defendants knew or should have known that it was a prized target for hackers; and (2) reasonable and adequate security protocols to promptly detect the unauthorized intrusion into and removal of PII/PHI from its provider database pertaining to nearly 12 million Data Breach victims.

11. Armed with PII/PHI, hackers can sell the PII/PHI to other thieves or misuse themselves to commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, open financial accounts, and open credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in another person's name; give false information to police during an arrest; or engage in medical fraud that can result in a harmful misdiagnosis to Plaintiff and Class members.

12. As a result of Defendants' willful failure to prevent the Data Breach, Plaintiff and Class members are more susceptible to identity theft and have experienced, will continue to experience, and face an increased risk of financial harms, in that they are at substantial risk of identity theft, fraud, and other harm.

PARTIES

13. Plaintiff Misty Marler is a resident and citizen of Orange County, California. Plaintiff is a customer of Quest Diagnostics, having used Quest Diagnostics at the Camino De Los Mares and Talega locations in San Clemente in Orange County, California. As a result of Defendants' actions, Plaintiff has been injured and has financial losses and will be subject to a substantial risk for further identity theft due to Defendants' Data Breach. As a further result of Defendants' actions, Plaintiff is contemplating purchasing credit monitoring and taking other measures to protect herself

from identity theft and fraud. Plaintiff believed, at the time of using Quest Diagnostics, that it would maintain the privacy and security of her PII/PHI. Plaintiff further believes she paid a premium to Quest Diagnostics for its data security. Plaintiff would not have used Quest Diagnostics had she known that it would expose, or allow to be exposed, her PII/PHI, making it available to unauthorized parties.

14. Defendant Quest Diagnostics Inc. is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

15. Based on information and belief, Defendant Optum360 Services, Inc. is a Delaware corporation with its principal place of business in Eden Praire, Minnesota.

16. Defendant American Medical Collection Agency is a business with its principal place of business in Elmsford, New York.

17. The true names and/or capacities, whether individual, corporate, partnership, associate or otherwise, of the Defendants herein designated as Does 1 to 100 are unknown to Plaintiff at this time who, therefore, sues said Defendants by fictitious names. Plaintiff alleges that each named Defendant herein designated as Does is negligently, willfully or otherwise legally responsible for the events and happenings herein referred to and proximately caused damages to Plaintiffs as herein alleged. Plaintiff will seek leave of Court to amend this Complaint to insert the true names and capacities of such Defendants when they have been ascertained and will further seek leave to join said Defendants in these proceedings.

18. Plaintiff is informed and believe and thereon alleges that at all times mentioned herein, Does were agents, servants, employees, partners, distributors or joint ventures of each other and that in doing the acts herein alleged, were acting within the course and scope of said agency, employment, partnership, or joint venture. Each and every Defendant aforesaid was acting as a principal and was negligent or grossly negligent in the selection, hiring and training of each and every other Defendant or ratified the conduct of every other Defendant as an agent, servant, employee or joint venture.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). This lawsuit is a class action with an amount in controversy over $5 million, involving over 100 proposed class members, some of whom are from a different state than Defendants.

20. This Court may exercise personal jurisdiction over Defendants because they are registered to do business and/or conduct business in California, and the wrongful acts alleged in this complaint were committed in California, among other venues.

21. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and Quest Diagnostics has at least 33 facilities in the State of California, and Defendants are subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

22. Beginning around August 1, 2018, unauthorized parties accessed the AMCA system that contained Plaintiff's and Class members' PII and PHI. Plaintiff and Class members are customers who paid and provided their PII and PHI to Quest Diagnostics in exchange for diagnostic and medical services. Quest Diagnostics provided Plaintiff and Class members' PII and PHI to Optum360 who in turn provided that information to AMCA for billing and collection purposes.

23. For more than six months, unauthorized parties maintained uninterrupted access to the AMCA system, containing the PII and PHI of nearly 12 million customers of Quest Diagnostics.

24. According to AMCA, a third-party credit card companies discovered the Data Breach and informed AMCA who confirmed the Data Breach after an internal review. Based on information and belief, AMCA learned about the Data Breach on or around March 30, 2019.

25. AMCA waited until May 14, 2019, to inform Quest Diagnostics and Optum360 of the Data Breach, who then waited more than two weeks to inform Plaintiff and Class members, only doing so through a June 3, 2019 SEC filing.

26. As a result, unauthorized parties have accessed and acquired Plaintiff and Class members' PII and PHI, including, but not limited to, their personal information (e.g. Social Security Numbers), financial information (credit card numbers and bank account information), and medical information.

27. Quest Diagnostics makes numerous promises to its customers that it will maintain the security and privacy of their personal information. For instance, in its Notice of Privacy Practices, Quest Diagnostics promises its customers that it is "committed to protecting the privacy of your identifiable health information."

28. Quest Diagnostics also acknowledges the following:

> Quest Diagnostics is required by law to maintain the privacy of your PHI. We are also required to provide you with this Notice of our legal duties and privacy practices upon request. It describes our legal duties, privacy practices and your patient rights as determined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). We are required to follow the terms of this Notice currently in effect. We are required to notify affected individuals in the event of a breach involving unsecured protected health information. PHI is stored electronically and is subject to electronic disclosure. This Notice does not apply to non-diagnostic services that we perform such as certain drugs of abuse testing services and clinical trials testing services.

29. Quest Diagnostics also ensures its customers it will only use their PII and PHI for certain limited purposes, such as "for treatment, payment, or healthcare operations purposes and for other purposes permitted or required by law." Quest Diagnostics further provides the following:

> need your written authorization to use or disclose your health information for any purpose not covered by one of the categories below. Subject to compliance with limited exceptions, we will not use or disclose psychotherapy notes, use or disclose your PHI for marketing purposes or sell your PHI, unless you have signed an authorization. You may revoke any authorization you sign at any time. If you revoke

> your authorization, we will no longer use or disclose your health information for the reasons stated in your authorization except to the extent we have already taken action based on your authorization.

30. By failing to protect Plaintiff and Class member's PII and PHI, and by allowing the Data Breach to occur, Quest Diagnostics broke these privacy promises.

31. To date, Defendants have not yet provided a Notice of Data Breach and have not adequately explained how the Data Breach occurred and why it took a third party to inform it of the Data Breach.

B. Personally Identifiable Information/Protected Health Information

32. PII/PHI is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners.

33. PII/PHI is information that can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and biometric records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

34. PII/PHI does not include only data that can be used to directly identify or contact an individual (e.g., name, e-mail address), or personal data that is especially sensitive (e.g., Social Security number, bank account number, payment card numbers).

35. PHI—like the type disclosed in the breach—is particularly valuable for cybercriminals. According to SecureWorks (a division of Dell Inc.), "[i]t's a well known truism within much of the healthcare data security community that an individual healthcare record is worth more on the black market ($50, on average) than a U.S.-based credit card and personal identity with social security number combined." The reason is that thieves "[c]an use a healthcare record to submit false medical claims (and thus obtain free medical care), purchase prescription medication, or resell the record on the black market."

36. Similarly, the FBI Cyber Division, in a April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

37. Given the nature of the Data Breach, it is foreseeable that the compromised PII/PHI will be used to access Plaintiff and the Class members' financial accounts, thereby providing access to additional PII/PHI or personal and sensitive information. Therefore, the compromised PII/PHI in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[1] For example, different PII/PHI elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.

38. Further, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."[2]

39. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity

[1] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report 35-38 (Dec. 2010) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf> [as of June 24, 2017].

[2] Fed. Chief Information Officers Council, Recommendations for Standardized Implementation of Digital Privacy Controls (Dec. 2012) pp. 7-8.

thieves as it allows them to access users' other accounts particularly when they have easily-decrypted passwords and security questions.

40. The PII/PHI Defendants exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names, obtaining protected health information, and/or committing medical fraud.

41. Unfortunately for Plaintiff and Class members, a person whose PII/PHI has been compromised may not fully experience the effects of the breach for years to come:

> [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.[3]

42. Accordingly, Plaintiff and Class members will bear a heightened risk of injury for years to come. Identity theft is one such risk and occurs when an individuals' PII/PHI is used without his or her permission to commit fraud or other crimes.[4]

43. According to the Federal Trade Commission, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[5]

---

[3] G.A.O., Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007) <http://www.gao.gov/assets/270/262904.html.> [as of June 24, 2017].

[4] Fed. Trade Comm'n, Taking Charge: What To Do If Your Identity Is Stolen (April 2013) <https://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf> [as of June 24, 2017].

[5] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (March 2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> [as of June 24, 2017].

C. HIPAA Provides Guidelines on How Healthcare Providers Must Secure Patients' Protected Health Information

44. As a healthcare provider, Defendants are subject to the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "Privacy and Security Rules").

45. The Privacy and Security Rules establish a national set of standards for the protection of "individually identifiable health information" that is held or transmitted by a health care provider, which HIPAA refers to as "protected health information."

46. Pursuant to HIPAA, Defendants must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI.

47. HIPAA imposes general security standards that Defendants must follow, including:

a. Ensuring the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits, 45 C.F.R. § 164.306(a);

b. Protecting against any reasonably anticipated threats or hazards to the security or integrity of such information, 45 C.F.R. § 164.306(a);

c. Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA, 45 C.F.R. § 164.306(a); and

d. Reviewing and modifying the security measures implemented under HIPAA as needed to continue provision of reasonable and appropriate protection of electronic protected health information, 45 C.F.R. § 164.306(e).

48. From a technical standpoint, HIPAA requires Defendants to, among other things:

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

b. Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed, 45 C.F.R. § 164.312(d); and

c. Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network, 45 C.F.R. § 164.312(e).

49. The HIPAA Security Rule requires Defendants to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. 45 CFR 164.316(a). These policies and procedures must be maintained in written form. 45 CFR 164.316(b)(1)(i).

50. The HIPAA Security Rule requires covered entities to maintain a written record of any action, activity, or assessment required to be documented by the HIPAA Security Rule. 45 CFR 164.316(b)(1)(ii).

51. The HIPAA Security Rule requires covered entities to review documentation periodically and update it as needed, in response to environmental or operational changes affecting the security of the electronic protected health information. 45 CFR 164.316(b)(1)(iii).

52. Under the HIPAA Privacy Rule, Defendants may not use or disclose PHI or confidential medical information except as expressly permitted. 45 CFR 164.502(a).

D. The HITECH Act Provides Additional Guidelines on How Healthcare Providers Must Secure Patients' Protected Health Information

53. The HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub.L. 111–5), promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act

addresses the privacy and security concerns associated with the electronic transmission of health information.

54. The HITECH Act provides lucrative financial incentives, and the avoidance of penalties, to healthcare entities such as Defendants for demonstrating the meaningful use, interoperability, and security of electronic health information. Achieving meaningful use requires compliance with objectives, measures and certification and standards criteria. The Electronic Health Records ("EHR") Incentive Program requires compliance with the objective to protect electronic health information. A Core Measure to determine compliance with the objective is conducting or reviewing a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) (the HIPAA Security Rule) and implementing security updates as necessary and correcting identified security deficiencies as part of its risk management process.

55. Upon information and belief, Defendants implanted a rushed and substandard EHR infrastructure in order to, in part, obtain millions of dollars in lucrative financial incentives, as well as the avoidance of penalties, despite knowing they were ill-equipped and unprepared to safely store and meaningfully use electronic health records and electronic health information in a secure manner consistent with regulations and industry standards.

E. Defendants are Subject To Other Federal and State Laws and Regulations That Provide Guidelines on the Practices It Should Have Implemented To Secure Patients' Protected Health Information

56. Section 5(a) of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, prevents Defendants from using "unfair or deceptive acts or practices in or affecting commerce." The FTC has found that inadequate data privacy and cybersecurity practices can constitute unfair or deceptive practices that violate § 5.

57. The state of California generally prohibits healthcare providers from disclosing a patient's confidential medical information without prior authorization. The California Confidentiality of Medical Information Act ("CMIA") (Cal. Civ. Code §

56.10(a)) states that "a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or enrollee or subscriber of a health care service plan without first obtaining an authorization except as provided in subdivision (b) or (c)." See also Cal. Civ. Code §§ 1798.80, et seq.

58. In addition to their obligations under federal and state laws and regulations, Defendants owed a common law duty to Plaintiffs and Class members to protect PII/PHI entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

59. Defendants further owed and breached its duty to Plaintiffs and the Class to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems (e.g. 45 CFR §§ 164.308(a), 164.306(d), 164.312, The Office for Civil Rights July 14, 2010 Guidance on Risk Analysis Requirements under the HIPAA Security Rule, etc.).

60. As a direct and proximate result of Defendants' reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiff's and Class members' PII/PHI, and Defendants' failure to properly and timely notify Plaintiff and Class members, Plaintiff and Class members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

a. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;

b. money and time lost as a result of fraudulent access to and use of their financial accounts;

c. loss of use of and access to their financial accounts and/or credit;

d. money and time expended to avail themselves of assets and/or credit

frozen or flagged due to misuse;

e. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

h. costs and lost time obtaining credit reports in order to monitor their credit records;

i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;

j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

k. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;

l. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

m. loss of the opportunity to control how their personal information is used; and

n. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendants fail to undertake appropriate, legally required steps to protect the personal information in its possession.

61. The risks associated with identity theft are serious. "While some identity

theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[6]

62. Further, criminals often trade stolen PII/PHI on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII/PHI on the internet, thereby making such information publicly available.

CLASS ACTION ALLEGATIONS

63. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

A. Nationwide Class

64. Plaintiff brings all claims on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows:

> *All persons in the United States whose PII/PHI was compromised as a result of the Data Breach.*

B. California Sub-Class

65. Plaintiff brings all claims on behalf of a proposed California Sub-Class, defined as follows:

> *All persons in the state of California whose PII/PHI was compromised as a result of the Data Breach.*

66. Excluded from the above Classes are Defendants, any entity in which Defendants have a controlling interest or that have a controlling interest in Defendants, and Defendants' legal representatives, assignees, and successors. Also excluded are the Judge to whom this case is assigned and any member of the Judge's immediate family.

67. **Numerosity:** The Nationwide Class is so numerous that joinder of all

[6] True Identity Protection: Identity Theft Overview, ID Watchdog <http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf> [as of Sept. 23, 2016].

members is impracticable. Based on information and belief, the Nationwide Class includes nearly 12 million individuals from across the country who had their PII/PHI compromised, stolen, and published during the Data Breach. The parties will be able to identify the exact size of the class through discovery and Defendants' own documents.

68. **Commonality:** There are numerous questions of law and fact common to Plaintiff and the Nationwide Class including, but not limited to, the following:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants owed a duty to Plaintiff and members of the Nationwide Class to adequately protect their personal information;
- whether Defendants breached their duties to protect the personal information of Plaintiff and Nationwide Class members;
- whether Defendants knew or should have known that its data security systems, policies, procedures, and practices were vulnerable;
- whether Plaintiff and Nationwide Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of PII/PHI;
- whether Defendants violated state consumer protection statutes; and
- whether Plaintiff and Nationwide Class members are entitled to equitable relief including injunctive relief.

69. **Typicality:** Plaintiff's claims are typical of the claims of the Nationwide Class members. Plaintiff, like all proposed Nationwide Class members, had their personal information compromised in the Data Breach.

70. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Nationwide Class. Plaintiff has no interests that are averse to, or in conflict with, the Nationwide Class members. There are no claims or defenses that are unique to Plaintiff. Likewise, Plaintiff has retained counsel experienced in class action and complex litigation, including data breach litigation, and have sufficient resources to prosecute

this action vigorously.

71. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Nationwide Class predominate over any questions which may affect only individual Nationwide Class members.

72. **Superiority:** The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

73. Absent a class action, the majority Nationwide Class members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

74. **Risks of Prosecuting Separate Actions:** Plaintiff's claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendants. Defendants continue to maintain the PII/PHI of Nationwide Class members and other individuals, and varying adjudications could establish incompatible standards with respect to its duty to protect individuals' personal information; and whether the injuries suffered by Nationwide Class members are legally cognizable, among others. Prosecution of separate action by individual class members would also create a risk of individual adjudications that would be dispositive of the interests of other class members not parties to the individual adjudications, or substantially impair or impede the ability of class members to protect their interests.

75. **Injunctive Relief:** In addition, Defendants have acted and/or refused to act on grounds that apply generally to the Nationwide Class, making injunctive and/or

declaratory relief appropriate with respect to the class under Federal Rule of Civil Procedure 23(b)(2). Defendants continue to (1) maintain the personally identifiable information of Nationwide Class members, (2) fail to adequately protect their personally identifiable information, and (3) violate their rights under numerous state consumer protection laws and other claims alleged herein.

FIRST CAUSE OF ACTION

Negligence

(On Behalf of the Nationwide Class Against Defendants)

76. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

77. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

78. Plaintiff and Nationwide Class members were required to provide Defendants with their PII/PHI. Defendants collected and stored this information including their names, Social Security numbers, payment card information, checking account and routing numbers, insurance provider information, salary information, dates of birth, addresses, and phone numbers.

79. Defendants had a duty to Plaintiff and Nationwide Class members to safeguard and protect their PII/PHI.

80. Defendants assumed a duty of care to use reasonable means to secure and safeguard this PII/PHI, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

81. Defendants have full knowledge about the sensitivity of Plaintiff and Nationwide Class members' PII/PHI, as well as the type of harm that would occur if such PII was wrongfully disclosed.

82. Defendants have a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with user PII/PHI data.

83. Defendants breached their duty of care by failing to secure and safeguard the PII of Plaintiff and Nationwide Class members. Defendants negligently stored

and/or maintained its data security systems, and published that information on the Internet.

84. Further, Defendants by and through their above negligent actions and/or inactions, breached their duties to Plaintiff and Nationwide Class members by failing to design, adopt, implement, control, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Nationwide Class members' PII/PHI within their possession, custody and control.

85. Defendants further breached their duty to Plaintiff and Nationwide Class members by failing to comply with the California Confidentiality of Medical Information Act, Consumers Legal Remedies Act, the Customer Record's Act, the Gramm-Leach-Bliley Act, and other state and federal laws designed to protect Plaintiff and Class members from the type of harm they here have suffered. Such a breach by Defendants constitutes negligence per se.

86. Plaintiff and the other Nationwide Class members have suffered harm as a result of Defendants' negligence. These victims' loss of control over the compromised PII subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

87. It was reasonably foreseeable – in that Defendants knew or should have known – that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Nationwide Class members' PII/PHI would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII/PHI, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

88. But for Defendants' negligent and wrongful breach of their responsibilities and duties owed to Plaintiff and Nationwide Class members, their PII/PHI would not have been compromised.

///

89. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Nationwide Class members' PII/PHI, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm for which they are entitled to compensation. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

90. Plaintiff and Nationwide Class members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION

Violation of California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, et seq.

(On Behalf of the Nationwide Class and California Sub-Class Against Defendants)

91. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

92. California's Confidentiality of Medical Information Act ("CMIA") requires a healthcare provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101. "Every provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." *Id.*

93. The CMIA further requires that "[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information." Cal. Civ. Code § 56.101(b)(1)(A).

94. Plaintiffs, Nationwide Class members, and California Sub-Class members are "patient[s]," "whether or not still living, who received health care services from a

provider of health care and to whom medical information pertains" pursuant to § 56.05(k) of the CMIA.

95. Quest Diagnostics is a "provider of healthcare" pursuant to § 56.05(m) of the CMIA "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information."

96. Quest Diagnostics is subject to the requirements and mandates of the CMIA.

97. The PHI of Plaintiffs, Nationwide Class members, and California Sub-Class members compromised in the Data Breach constitutes "medical information" maintained in electronic form pursuant to § 56.05(j) of the CMIA.

98. Defendants violated § 56.36(b) of the CMIA by negligently maintaining, preserving, storing and releasing the PHI of Plaintiffs, Nationwide Class members, and California Sub-Class members, and failing to protect and preserve the integrity of the PHI of Plaintiffs and California Subclass members.

99. Plaintiffs, Nationwide Class members, and California Sub-Class members did not authorize Quest Diagnostics disclosure and release of their PHI that occurred in the Data Breach.

100. As a result of the Data Breach, the PHI of Plaintiffs, Nationwide Class members, and California Sub-Class members was compromised when it was acquired and accessed by unauthorized parties.

101. Quest Diagnostics violated the CMIA by negligently (1) failing to implement reasonable administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiffs' and California Subclass members' PHI; (2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs, Nationwide Class members, and California Sub-Class members' PHI; (3) failing to use reasonable authentication procedures to track PHI in case of a security breach; and (4) allowing undetected and unauthorized

access to servers, networks and systems where Plaintiffs, Nationwide Class members, and California Sub-Class members' PHI was kept, all in violation of the CMIA.

102. Quest Diagnostics failure to implement adequate data security measures to protect the PHI of Plaintiffs, Nationwide Class members, and California Sub-Class members was a substantial factor in allowing unauthorized parties to access Quest Diagnostics computer systems and acquire the PHI of Plaintiffs and California Subclass members.

103. As a direct and proximate result of Quest Diagnostics violation of the CMIA, Quest Diagnostics allowed the PHI of Plaintiffs, Nationwide Class members, and California Sub-Class members to: (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed and acquired by unauthorized parties in order to, on information and belief, view, mine, exploit, use, and/or profit from their PHI, thereby breaching the confidentiality of their PHI. Plaintiffs and California Subclass members have accordingly sustained and will continue to sustain actual damages as set forth above.

104. Plaintiffs, individually and on behalf of California Subclass members, seek actual and statutory damages pursuant to § 56.36(b)(1) of the CMIA.

105. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23, Civil Code § 56.35, and California Code of Civil Procedure § 1021.5.

FOURTH CAUSE OF ACTION

N.Y. Gen. Bus. Law § 349

(On Behalf of the Nationwide Class Against Defendants)

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

107. 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 PII/PHI 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 PII/PHI, 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).

108. 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 PII/PHI.

109. 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.

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

111. Plaintiff seeks 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. *Id.*

112. 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 PII/PHI entrusted to them, as detailed herein.

113. 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.

FOURTH CAUSE OF ACTION

Violation of California Consumers Legal Remedies Act, California Civil Code § 1750, *et seq.*

(On Behalf of the Nationwide Class and California Sub-Class Against Defendants)

114. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

115. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq.* This cause of action does not seek monetary damages at this time but is limited solely to injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendants with notice required by California Civil Code § 1782.

///

116. Plaintiff and Nationwide Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

117. Plaintiff, Nationwide Class members, and Defendants have engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

118. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct was undertaken by Defendant was likely to deceive consumers.

119. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

120. Defendants violated this provision by representing that they took appropriate measures to protect Plaintiff's and the Nationwide Class members' PII/PHI. Additionally, Defendants improperly handled, stored, or protected either unencrypted or partially encrypted data.

121. As a result, Plaintiff and Nationwide Class members were induced to enter into a relationship with Defendants and provide their PII/PHI.

122. As a result of engaging in such conduct, Defendants have violated Civil Code § 1770.

123. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks an order of this Court that includes, but is not limited to, an order enjoining Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

124. Plaintiff and Nationwide Class members suffered injuries caused by Defendants' misrepresentations, because they provided their PII/PHI believing that Defendants would adequately protect this information.

125. Plaintiff and Nationwide Class members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

///

126. The unfair and deceptive acts and practices of Defendants, as described above, present a serious threat to Plaintiff and members of the Nationwide Class.

FOURTH CAUSE OF ACTION

Violation of Unfair Competition Law,

California Business and Professional Code Section 17200, *et seq*.

(On Behalf of the Nationwide Class and California Sub-Class Against Defendants)

127. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

128. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

129. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

130. By reason of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiff and Nationwide Class members' PII/PHI, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

131. Defendants' business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII/PHI of consumers has been compromised for all to see, use, or otherwise exploit.

132. Defendants' practices were unlawful and in violation of Civil Code § 1798 *et seq*. because Defendants failed to take reasonable measures to protect Plaintiff's and the Nationwide Class members' PII/PHI.

133. Defendants' business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII/PHI they provide to Defendants will remain private and secure, when in fact it was not private and secure.

134. Plaintiff and the Nationwide Class members suffered (and continue to

suffer) injury in fact and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII/PHI.

135. Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Nationwide Class members' PII/PHI also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 *et seq*., in that Defendants' conduct was substantially injurious to Plaintiff and Nationwide Class members, offensive to public policy, immoral, unethical, oppressive and unscrupulous; the gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct.

136. But for Defendants' misrepresentations and omissions, Plaintiff and Nationwide Class members would not have provided their PII/PHI to Defendants or would have insisted that their PII/PHI be more securely protected.

137. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Nationwide Class members' PII/PHI, they have been injured: (1) the loss of the opportunity to control how their PII/PHI is used; (2) the diminution in the value and/or use of their PII/PHI entrusted to Defendants; (3) the compromise, publication, and/or theft of their PII/PHI; and (4) costs associated with monitoring their PII/PHI, amongst other things.

138. Plaintiff takes upon herself enforcement of the laws violated by Defendants in connection with the reckless and negligent disclosure of PII/PHI. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiff by forcing him to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

///

///

FIFTH CAUSE OF ACTION

Violation of California Customer Records

Act, California Civil Code § 1798.80 et.seq.

(On Behalf of the Nationwide Class and California Sub-Class Against Defendants)

139. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

140. "[T]o ensure that personal information about California residents is protected," Civil Code section 1798.81.5 requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

141. Defendants own, maintain, and license personal information, within the meaning of section 1798.81.5, about Plaintiff and the Nationwide Class.

142. Defendants violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiff and Nationwide Class members' personal information.

143. As a direct and proximate result of Defendants' violations of section 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

144. As a direct and proximate result of Defendants' violations of section 1798.81.5 of the California Civil Code, Plaintiff and the Nationwide Class members suffered the damages described above including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personally identifying information.

145. Plaintiff and the Nationwide Class members seek relief under section 1798.84 of the California Civil Code including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

SIXTH CAUSE OF ACTION

Breach of Contract

(On Behalf of the Nationwide Class Against Defendants)

146. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

147. Plaintiff and Class members entered into a contract with Defendants for the provision of title insurance or other closing services.

148. The terms of Defendants' privacy policy are part of the contract.

149. Plaintiff and Class members performed substantially all that was required of them under their contract with Defendants, or they were excused from doing so.

150. Defendants failed to perform its obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs and Class member's information and documents.

151. As a direct and proximate result of Defendants' breach of contract, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received title insurance or other closing services that were less valuable than described in their contracts. Plaintiff and 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.

152. Also, as a result of Defendants' breach of contract, Plaintiff and Class members have suffered actual damages resulting from the exposure of their personal information, and they remain at imminent risk of suffering additional damages in the future.

153. Accordingly, Plaintiff and 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.

///

///

///

SEVENTH CAUSE OF ACTION

Breach of Implied Contract

(On Behalf of the Nationwide Class Against Defendants)

154. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

155. Plaintiff brings this cause of action on behalf of the Class and to the extent necessary.

156. 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.

157. 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, Plaintiff 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 Plaintiff and the Class to pay for adequate and reasonable data security practices.

158. Plaintiff and the Class 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.

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

160. Defendants breached their implied contracts with Plaintiff and the Class 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.

161. As a direct and proximate result of Defendants' breaches of their implied

contracts, Plaintiff and the Class sustained actual losses and damages as described herein

EIGHTH CAUSE OF ACTION

Unjust Enrichment

(On Behalf of the Nationwide Class Against Defendants)

162. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

163. Defendants received a benefit from Plaintiff and the Class in the form of payments for title insurance or other closing services.

164. The benefits received by Defendants were at Plaintiff's and the Class's expense.

165. The circumstances here are such that it would be unjust for Defendants to retain the portion of Plaintiff's and the Class's payments that should have been earmarked to provide adequate privacy, security, and confidentiality safeguards for Plaintiffs and Class members' personal information and documents.

166. Plaintiff and the Class seek disgorgement of Defendants' ill-gotten gains.

NINTH CAUSE OF ACTION

Invasion of Privacy

(On Behalf of the Nationwide Class Against Defendants)

167. Plaintiff re-alleges the paragraphs above as if fully set forth herein.

168. Plaintiff brings this claim on behalf of himself and the Nationwide Class.

169. Plaintiff and Class members have a legally protected privacy interest in their PII/PHI that Defendants required them to provide and allow them to store.

170. Plaintiff and Class members reasonably expected that their PII/PHI would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

171. Defendants unlawfully invaded the privacy rights of Plaintiffs and Class members by (a) failing to adequately secure their PII/PHI from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII/PHI to

unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII/PHI to unauthorized parties without the informed and clear consent of Plaintiffs and Class members. This invasion into the privacy interest of Plaintiff and Class members is serious and substantial.

172. In failing to adequately secure Plaintiff's and Class members' PII/PHI, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiff and Class members.

173. Defendants violated Plaintiff's and Class members' right to privacy under the common law as well as under state and federal law, including, but not limited to, the California Constitution, Article I, Section I.

174. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class members' PII/PHI has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and the proposed Class have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

PRAYER FOR RELIEF

175. WHEREFORE, Plaintiff requests that the Court enter a judgment awarding the following relief:

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Nationwide Class requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Injunctive relief requiring Defendants to (1) strengthen their data security systems that maintain personally identifying information to comply with the applicable state laws alleged herein (including, but not limited to, the California Customer Records Act) and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on

Defendants' systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

c. An order requiring Defendant to pay all costs associated with class notice and administration of class-wide relief;

d. An award to Plaintiff and all Nationwide Class members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

e. An award to Plaintiff and all Nationwide Class members credit monitoring and identity theft protection services;

f. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

g. An order requiring Defendants to pay pre-judgment and post-judgment interest, as provided by law or equity; and

h. Such other or further relief as the Court may allow.

Dated: June 3, 2019

Respectfully submitted,

ROBINSON CALCAGNIE, INC.

/s/ Daniel S. Robinson

Daniel S. Robinson
drobinson@robinsonfirm.com
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues in this action so triable of right.

Dated: June 3, 2019

Respectfully submitted,

ROBINSON CALCAGNIE, INC.

/s/ Daniel S. Robinson

Daniel S. Robinson
drobinson@robinsonfirm.com
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288