IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
SPARTANBURG DIVISION

Shawn Peticos, on behalf of himself and all others similarly situated, Plaintiff, v. Oral and Maxillofacial Surgery Associates, P.A., Defendant.	C.A. No.: _____

NOTICE OF REMOVAL

Pursuant to 28 U.S.C. §§ 1441(a), (b) and § 1446, Defendant Oral and Maxillofacial Surgery Associates, P.A. ("Defendant"), files this Notice of Removal to the United States District Court for the District of South Carolina, Spartanburg Division. Removal is proper based on the following grounds:

1. Plaintiff Shawn Peticos, on behalf of himself and all others similarly situated, initiated a civil action captioned *Shawn Peticos, et al. v. Oral and Maxillofacial Surgery Associates, P.A.*, C. A. No. 2020-CP-42-03041 in the Court of Common Pleas of Spartanburg County, South Carolina.

2. Defendant was served with a copy of the Summons and Complaint on October 26, 2020. The documents attached hereto as "Exhibit A" constitute all the process and pleadings received by Defendant in this action to date.

3. Upon information and belief, and according to the Complaint's allegations, Plaintiff is a resident and citizen of the State of North Carolina. (*See* Complaint at ¶ 8.)

4. Oral and Maxillofacial Surgery Associates, P.A. is incorporated in the State of South Carolina and its principal place of business is in the State of South Carolina. (*See id.* at ¶ 9.) Accordingly, Defendant is a citizen of the State of South Carolina for jurisdictional purposes.

5. Thus, there is complete diversity of citizenship between Plaintiff and Defendant in this action.

6. The amount in controversy in this action, exclusive of interest and costs, exceeds $75,000. The Complaint contains the following five causes of action: (1) negligence; (2) breach of implied contract; (3) violation of consumer identity theft protection act; (4) unjust enrichment; and (5) injunctive and declaratory relief. Plaintiff seeks unspecified damages, costs and expenses, and attorneys' fees. (*See* Complaint at ¶ 124n, o, p.) Furthermore, Plaintiff failed to plead that his damages were less than $75,000 in accordance with S.C.R. Civ. P. 8(a). Based upon the nature of the claims and damages sought, Plaintiff's allegations are adequate to establish an amount in controversy that exceeds $75,000.

7. In light of the preceding allegations, removal is proper under 28 U.S.C. § 1441. This Court has original jurisdiction over this action under 28 U.S.C. § 1332(a) because there is complete diversity of citizenship between the parties and the amount in controversy exceeds $75,000.

THE CLASS ACTION FAIRNESS ACT GRANTS THIS COURT JURISDICTION OVER THIS ACTION

8. As an additional basis for federal jurisdiction, this Court has original jurisdiction over this action under the Class Action Fairness Act of 2005 (codified in pertinent part at 28 U.S.C. §§ 1332(d) and 1453(b)) ("CAFA"), because: (i) the putative class consists of at least 100 proposed class members; (ii) the citizenship of at least one proposed class member is diverse from Defendant; and (iii) the amount in controversy, after aggregating the sum or value of each

proposed class member's claim, exceeds $5 million, exclusive of interest and costs. *See Dominion Energy, Inc. v. City of Warren Police & Fire Ret. Sys.*, 928 F.3d 325, 330 (4th Cir. 2019).

9. Plaintiff proposes certification of the following class: "[a]ll persons whose PII and PHI was compromised as a result of the Data Breach announced by OMSA beginning on or about February 21, 2020." (Complaint at ¶ 58.) Plaintiff alleges that the numerosity requirement under Federal Rule of Civil Procedure 23(a)(1) is met as the Data Breach implicated more than 35,000 persons. (*See id.* at ¶ 62.) Accordingly, the Proposed Class consists of at least 100 potential putative class members, and the requirement under 28 U.S.C. § 1332(d)(5) is satisfied.

10. As alleged and previously stated in this Notice of Removal, Defendant is incorporated in the state of South Carolina and its principal place of business is in the state of South Carolina. (*See id.* at ¶ 9.)

11. According to the Complaint's allegations, Plaintiff as the named Plaintiff of the putative class is not a resident of South Carolina. (*See id.* at ¶ 8.) Thus, 28 U.S.C. § 1332(d)(2)'s diversity of citizenship requirement, minimal diversity between at least one proposed class member and Defendant, is met.

12. Plaintiff requests on his own behalf and on behalf of the Proposed Class, a mandatory injunction, damages, costs and expenses, and attorneys' fees. (*See id.* at ¶ 124n, o, p.) Such liability is predicated upon Plaintiff's allegations that Defendant breached a duty by failing to properly and adequately safeguard Plaintiff's and Proposed Class Members' personally identifiable information ("PII") and protected health information ("PHI"). As a result of the alleged breach, Plaintiff seeks recovery of at least $3,000 per violation under the consumer identity theft protection act, plus attorneys' fees and costs for himself and each member of the Proposed Class. (*See id*. at ¶ 106.) This request puts the amount in controversy at over $100 million ($3,000 x 35,000 putative

class members). Accepting Plaintiff's factual allegations as true and legal allegations as correct solely for evaluating the amount in controversy, based on the number of putative class members as well as the damages and other relief sought, the amount in controversy requirements under 28 U.S.C. §§ 1332(d)(2) and 1332(d)(6) are met.

13. A primary purpose of CAFA is to provide federal court consideration of interstate cases of national importance under diversity jurisdiction. *See* Class Action Fairness Act of 2005, Pub. L No. 109-2, § 2(b)(2), 119 Stat. 4 (2005).

14. Plaintiff alleges that data breaches and cyberattacks in the healthcare sector in particular are a matter of national importance. Plaintiff supports this allegation by including in the Complaint numerous statistics of data breaches in the United States over the past few years. (*See* Complaint at ¶ 20, 21, 22, 23, 24.)

15. In the Complaint, Plaintiff proceeds to raise matters of national importance by alleging that Defendant either violated or failed to comply with multiple federal laws, regulations, and guidelines.

16. Plaintiff asserts that Defendant failed to comply with federal requirements and regulations under the Health Insurance Portability and Accountability Act ("HIPAA") in detail. (*See id.* at ¶ 17, 18, 19, 96(b)-(f).)

17. Plaintiff also states "[Defendant] **violated** Section 5 of the Federal Trade Commission Act by failing to use reasonable measures to protect patients' PII and PHI and not complying with applicable industry standards." (*Id.* at ¶ 78.) Additionally, Plaintiff alleges that Defendant failed to comply with other Federal Trade Commission guidelines related to data security practices. (*See id.* at ¶ 36, 37, 38, 39, 40.)

18. Further, Plaintiff alleges that Defendant failed to comply with national industry cybersecurity standards promulgated by the Department of Health and Human Services' Office for Civil Rights. (*See id.* at ¶ 42, 43, 45.)

19. In light of the preceding allegations, this Court has original jurisdiction over this action under 28 U.S.C. § 1332(d) because the putative class consists of at least 100 proposed class members; the citizenship of at least one proposed class member is diverse from Defendant; the amount in controversy, after aggregating the sum or value of each proposed class member's claim, exceeds $5 million, exclusive of interest and costs; and this is an interstate case of national importance.

20. Defendant submits this Notice of Removal without waiving any defenses to the claims asserted by Plaintiff and without conceding that Plaintiff has alleged claims upon which relief may be granted.

21. This Notice of Removal is filed with the Court within thirty (30) days of service of the Summons and Complaint, in accordance with 28 U.S.C. § 1446(b).

22. This Notice of Removal is signed pursuant to Rule 11 of the Federal Rules of Civil Procedure.

23. Written notice of the filing of this Notice of Removal will be given to Plaintiff, and together with a copy of the Notice of Removal and supporting papers, will be filed with the Clerk of Court for the County of Spartanburg, South Carolina.

WHEREFORE, Defendant gives notice that the referenced action pending in the Court of Common Pleas for Spartanburg County has been removed to the United States District Court for the District of South Carolina, Spartanburg Division.

Respectfully submitted,

By: s/ *T. Chase Samples*
T. Chase Samples (Fed. Bar No. 10824)
Email: Chase.Samples@jacksonlewis.com
Laura A. Ahrens (*Fed. Bar Admission Pending*)
Email: Laura.Ahrens@jacksonlewis.com
JACKSON LEWIS P.C.
15 South Main Street, Suite 700
Greenville, SC 29601
Phone: (864) 232-7000

Damon W. Silver, Esq.
(*Pro Hac Vice Admission Pending*)
Email: Damon.Silver@jacksonlewis.com
JACKSON LEWIS P.C.
666 Third Ave., 29th Floor
New York, NY 10017
Phone: (212) 545-4063

Jason C. Gavejian, Esq.
(*Pro Hac Vice Admission Pending)*
Email: Jason.Gavejian@jacksonlewis.com
JACKSON LEWIS P.C.
200 Connell Drive, Suite 2000
Berkeley Heights, NJ 07922
Phone: (908) 795-5139

ATTORNEYS FOR DEFENDANT

Dated: November 25, 2020

CERTIFICATE OF SERVICE

The undersigned certifies that a true and correct copy of the foregoing **DEFENDANTS' NOTICE OF REMOVAL TO FEDERAL COURT** was filed via ECF this 25th day of November, 2020, which automatically sends electronic notice, and *via* U.S. Mail and e-mail to:

Patrick Graves, Esq.
MORGAN & MORGAN
170 Meeting Street, Suite 110
Charleston, SC 29401
Email: pgraves@forthepeople.com

John A. Yanchunis, Esq.
Patrick A. Barthle, Esq.
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Email: jyanchunis@forthepeople.com
Email: pbarthle@forthepeople.com

Joel R. Rhine, Esq.
Martin A. Ramey, Esq.
RHINE LAW FIRM, P.C.
1612 Military Cutoff Rd., Suite 300
Wilmington, NC 28403
Email: jrr@rhinelawfirm.com
Email: mjr@rhinelawfirm.com

s/ *T. Chase Samples*

This 25th day of November, 2020.

4831-3457-4802, v. 4

EXHIBIT A

State Court Documents

STATE OF SOUTH CAROLINA IN THE COURT OF COMMON PLEAS

COUNTY OF SPARTANBURG 2020-CP-_____

Shawn Peticos, on behalf of himself and all others similarly situated,

Plaintiff,

v.

Oral and Maxillofacial Surgery Associates, P.A.,

Defendant.

SUMMONS

TO: ORAL AND MAXILLOFACIAL SURGERY ASSOCIATES, P.A.

YOU ARE HEREBY SUMMONED and required to answer the Complaint herein, a copy of which is herewith served upon you, and to serve a copy of your Answer to said Complaint upon the subscriber at his office at Morgan & Morgan, 170 Meeting Street, Suite 110, Charleston, South Carolina 29223 within thirty (30) days after the service hereof, exclusive of the day of such service, and if you fail to answer the Complaint within the aforesaid, judgment by default will be rendered against you for the relief demanded in the Complaint.

MORGAN & MORGAN

/s/ Patrick Graves, Esq.
Patrick Graves, SC Bar No.: 100369
170 Meeting Street
Suite 110
Charleston, SC 29401
Telephone: (843) 973-5180
Email: pgraves@forthepeople.com

September 4, 2020.

John A. Yanchunis*
Patrick A. Barthle*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
jyanchunis@forthepeople.com
pbarthle@forthepeople.com

Joel R. Rhine*
Martin A. Ramey*
RHINE LAW FIRM, P.C.
1612 Military Cutoff Rd., Suite 300
Wilmington, NC 28403
Telephone: (910) 772-9960
jrr@rhinelawfirm.com
mjr@rhinelawfirm.com

Attorneys for Plaintiff and the Putative Class

*Motions for *pro hac vice* admission to be filed

STATE OF SOUTH CAROLINA

COUNTY OF SPARTANBURG

IN THE COURT OF COMMON PLEAS

2020-CP-_____

Shawn Peticos, on behalf of himself and all others similarly situated,

Plaintiff,

v.

Oral and Maxillofacial Surgery Associates, P.A.,

Defendant.

CLASS ACTION COMPLAINT
(JURY TRIAL DEMANDED)

Plaintiff Shawn Peticos, by and through his undersigned counsel, brings this class action lawsuit against Defendant Oral and Maxillofacial Surgery Associates, P.A. (hereinafter "OMSA" or "Defendant") on behalf of himself and all others similarly situated, and alleges, based upon information and belief and the investigation of his counsel as follows:

INTRODUCTION

1. Incorporated in 1996, OMSA is an oral and maxillofacial surgery practice with two offices in Spartanburg, South Carolina and one office in Rutherfordton, NC. The practice provides services to patients in need of surgery to remove impacted wisdom teeth, to prepare for dental implants, and to perform corrective face and jaw surgery, among others.

2. On or about June 17, 2020, OMSA notified its current and former patients that someone had carried out a cyberattack on the practice's information systems on February 21, 2020 (the "Data Breach"). According to the Notice sent to OMSA's patients, it took the Defendant until April 22, 2020 to even detect the attack. (A true and correct copy of the Notice sent to Plaintiff is

attached hereto as Exhibit "A.")

3. According to the Notice, OMSA determined that the cyberattacker had gained access to files containing personal health information ("PHI") and/or personally identifiable information ("PII") of its patients.

4. Interestingly, although the Notice stated that the data exfiltrated in the attack only "contained one or multiple data elements of PHI and/or PII including names, X-ray and other treatment-related images, and/or dates of birth," OMSA offered to provide its patients with 12 months of free credit monitoring and related services. Plaintiff is informed and believes, and thereon alleges, that the stolen data also contained far more sensitive data than as stated by OMSA, given its offer of credit monitoring.

5. With the discovery of the attack some two months after it had occurred, it is evident that OMSA disregarded its duties toward patient privacy and confidentiality. Through its actions and omissions, OMSA intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failed to disclose that OMSA did not have adequately robust computer systems and security practices to safeguard PII and PHI; failed to take standard and reasonably available steps to prevent the Data Breach; failed to monitor and timely detect the Data Breach; and failed to provide Plaintiff and Class Members with prompt and accurate notice of the Data Breach.

6. As a result of Defendant's failure to implement and follow basic security procedures, PII and PHI is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and fraud.

7. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, breach of implied contract, unjust enrichment and violations of the South Carolina Consumer Fraud Act, and seeks to compel the Defendant to adopt reasonably sufficient security practices to safeguard PII and PHI that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

8. Plaintiff is a citizen and resident of Rutherford County, North Carolina. He is a former patient of OMSA.

9. OMSA is a duly incorporated South Carolina corporation with its main offices in this county.

JURISDICTION AND VENUE

10. This Court has jurisdiction over the Defendant, as it is headquartered in this state, operates two offices in this county, and maintains its computers, computer systems and patient records here.

11. Plaintiff and Class Members are patients of OMSA who received treatment and services from its dentists and surgeons located at one or more of OMSA's three offices in both South Carolina and North Carolina. As part of OMSA's initial patient intake procedures, patients are asked for their PII and PHI, which is then entered in various forms in OMSA's computers and computer systems. Such information is believed to be consulted and accessed by OMSA's providers and staff in the regular course of business and course of treatment of its patients. Through its business operations in this state, OMSA intentionally avails itself of the benefits of South Carolina residents and patients sufficient to render the exercise of jurisdiction by this Court just and proper.

12. Venue is proper in this Court because a substantial part of the events and omissions giving rise to this action occurred here and the Defendant is a resident of this county.

STATEMENT OF FACTS

A. The Data Breach

13. On or about February 21, 2020, an unauthorized person gained access to the computer systems maintained by OMSA. That access led to the exfiltration of one or more data sets containing sensitive information belonging to OMSA's patients.

14. The stolen data included personally identifiable information ("PII"), including names, X-ray and other treatment-related images, and/or dates of birth, of current and former patients. Because OMSA's intake forms request that patients provide sensitive information such as addresses, Social Security Numbers, etc., it is likely that the attack collected such data. Certainly, the concern was so comprehensive and deep that OMSA felt obligated to provide credit monitoring services for one year, something that would not have otherwise be required on the data that OMSA says was stolen, unless that data contained more sensitive information.

15. Even though the access occurred in February, it was not until four months later that OMSA notified its patients of the Data Breach.

16. The Notice of the breach sent by OMSA to Plaintiff Peticos stated, in relevant part:

June 17, 2020

What Happened

> We are writing to notify you that Oral and Maxillofacial Associates, P.A. (the "Practice") was victimized by a cyberattack (the "Incident"). We immediately commenced an investigation of the Incident with assistance from third party experts for the purpose of determining its scope, the impact on our information systems. and the identities of those the Incident may have affected.

On or about April 22, 2020, we determined that, on February 21, 2020, the cyberattacker may have accessed files on our systems that contain personal health information ("PHI") and/or personally identifiable information ("PII") that relates to you. We have not found any evidence that the information contacted in the affected files was misused as a result of the Incident.

What Information Was Involved

The files potentially accessed as a result of the Incident contained one or multiple data elements of PHI and/or PII including names, X-ray and other treatment-related images. and/or dates of birth.

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity. credit, and personal information.

As an added precaution, we have arranged for TransUnion to provide to you 12 months of free credit monitoring and related services. Please see the attached instructions on how to enroll. To receive these services, please be sure to enroll by **September 30, 2020**. Your activation code is: **(REDACTED)**

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since learning of the attack, we have taken a number of steps to further secure our systems. Specifically, we have, among other things: formatted our server and all impacted workstations; vetted and monitored all equipment attached to our network; and replaced operating systems and workstations that were compromised as a result of the Incident.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

If you have questions or concerns, please contact 855-917-3551 Monday through Friday 9am to 9pm Eastern Time. We sincerely apologize for this situation and any inconvenience it may cause you.

B. OMSA's Obligations to Keep PII and PHI Secure

17. Due to its business and operations, OMSA is obligated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to comply with a series of administrative, physical security, and technical security requirements in order to protect sensitive patient information. Among other things, the law mandates OMSA develop, publish, and adhere to a privacy practice.

18. As such, OMSA recognizes its obligations under HIPAA to safeguard and protect patient PHI and PII. Furthermore, it is well known that healthcare organizations have been the target of an increasing number of cyberattacks and must take adequate and reasonable steps to protect their systems from attack.

19. Moreover, under various federal and state laws, regulations, industry practices and common law, OMSA is bound to safeguard and protect the personal data of its patients to avoid unauthorized disclosure to third parties.

C. Prevalence of Cyberattacks and Susceptibility of the Healthcare Sector

20. Cyberattacks come in many forms. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a 40% increase in the number of data breaches from the previous year.[1] In 2017, a new record high of 1,579 breaches were reported, representing a 44.7% increase over 2016.[2]

21. In 2018, the healthcare sector reported the second largest number of breaches

---

[1] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at* https://www.idtheftcenter.org/surveys-studys (last visited September 3, 2020).

[2] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, available at https://www.idtheftcenter.org/2017-data-breaches/ (last visited September 3, 2020).

among all measured sectors and the highest rate of exposure per breach.[3] Healthcare related data is among the most sensitive and personally consequential when compromised. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident…came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[4] Almost 50% of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy.[5]

22. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82% of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[6] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security Numbers and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much

---

[3] Identity Theft Resource Center, 2018 End-of-Year Data Breach Report, *available at* https://www.idtheftcenter.org/2018-data-breaches/ (last visited September 3, 2020).

[4] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, March 3, 2010, https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited September 3, 2020).

[5] *Id.*

[6] HIMSS, 2019 HIMSS Cybersecurity Survey, https://www.himss.org/himss-cybersecurity-survey (last visited April 13, 2020).

monetizable information stored in their data centers."[7]

23. Indeed, the HIPAA Journal 2019 Healthcare Data Breach Report demonstrates an upward trend in health sector data breaches over the past 10 years, with 2019 reflecting more data breaches than any other year.[8] The year 2019 represented a 37.4% increase over breaches reported in 2018 with a total number of patient records exposed increasing from 13,947,909 in 2018 to 41,335,889.[9]

24. "Shockingly, the report disclosed that in 2019 alone, the healthcare records of 12.55% of the population of the United States were exposed, impermissibly disclosed, or stolen."[10]

25. As a healthcare provider, OMSA thus knew, or should have known, the importance of safeguarding patient PHI and PII entrusted to it and of the foreseeable consequences if its data security systems were breached, including the significant costs that would be imposed on its patients as a result of a breach. But OMSA failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

[7] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited September 3, 2020).

[8] HIPAA Journal, Healthcare Data Breach Statistics, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited September 3, 2020).

[9] *2019 Healthcare Data Breach Report*, HIPAA Journal, https://www.hipaajournal.com/2019-healthcare-data-breach-report/ (last visited September 3, 2020).

[10] *Report Reveals Worst State for Healthcare Data Breaches in 2019*, Info Security Group, February 14, 2020, https://www.infosecurity-magazine.com/news/report-healthcare-data-breaches-in/ (last visited September 3, 2020).

D. OMSA Acquires, Collects, and Stores Plaintiff's and Class Members' PII and PHI

26. OMSA acquires, collects, and stores a massive amount of protected health related information and other personally identifiable data on its patients.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, OMSA assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from unauthorized disclosure.

28. At all times relevant hereto, Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI. Plaintiff and Class Members relied on OMSA to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

E. The Value of Personally Identifiable Information and the Effects of Unauthorized Disclosure

29. OMSA was well aware that the PII and PHI it collects and maintains on patients is extremely sensitive, and of significant value to those who would use it for wrongful purposes.

30. Personally identifiable information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[11] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites.

31. While credit card information can sell for as little as $1-$2 on the black market, other more sensitive information can sell for as much as $363 according to the Infosec Institute.

---

[11] Federal Trade Commission, *Warning Signs of Identity Theft*, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited September 3, 2020).

PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

32. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security Number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

33. Moreover, it is not an easy task to change or cancel a stolen Social Security Number. An individual cannot obtain a new Social Security Number without significant paperwork and evidence of actual misuse. Even then, a new Social Security Number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[12]

34. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than

---

[12] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 3, 2020).

10x on the black market."[13] As explained above, the inclusion of PHI, such as the information exposed here, is even more valuable.

35. At all relevant times, OMSA knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security systems were breached, including, the significant costs that would be imposed on patients as a result of a breach.

F. OMSA Failed to Comply with FTC Guidelines

36. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

37. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[15] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any

---

[13] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited September 3, 2020).

[14] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited September 3, 2020).

[15] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited September 3, 2020).

security problems.

38. The FTC further recommends that companies not maintain PHI and PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[16]

39. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. OMSA failed to properly implement basic data security practices. OMSA's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

41. OMSA was always fully aware of its obligation to protect the PII of patients because of its position as a healthcare provider. OMSA was also aware of the significant repercussions that would result from its failure to do so.

G. OMSA Failed to Comply with Industry Standards

42. Data exfiltrated from healthcare providers continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a

---

[16] FTC, *Start With Security*, *supra* note 23.

number which continued to grow in 2018 (363 breaches).[17] The costs of healthcare data breaches are among the highest across all industries, topping $380 per stolen record in 2017 as compared to the global average of $141 per record.[18] As a result, both the government and private sector have developed industry best standards to address this growing problem.

43. The Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[19] DHHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience which require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of PHI and PII; (b) educating and training healthcare employees on how to protect PHI and PII; and (c) correcting the configuration of software and network devices.

44. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyberattacks, both because of the value of the individuals' PHI and PII they maintain and because as an industry they have been slow to adapt and respond to cybersecurity

---

[17] https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry; Identity Theft Resource Center, 2018 End of Year Data Brach Report, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last visited September 3, 2020).

[18] *Id.*

[19] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA Journal, November 1, 2018, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last visited September 3, 2020).

threats.[20] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of PHI and PII.

45. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, OMSA chose to ignore them. These best practices were known, or should have been known by OMSA, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of PII and PHI.

H. Plaintiff and Class Members Suffered Damages

46. The ramifications of Defendant's failure to keep patients' PII and PHI secure are long lasting and severe. Once stolen, fraudulent use of such information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[21]

47. The PII and PHI belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant, who did not obtain Plaintiff's or Class Members' consent to disclose such information to any other person as required by applicable law and industry standards.

48. Upon receiving the Notice, Plaintiff immediately took action to investigate whether the breach resulted in any fraud. Plaintiff contacted his creditors and reviewed his credit reports to determine if any fraudulent charges or activity appeared. Plaintiff continues to monitor his

---

[20] *See, e.g.,* https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry; https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref (last visited September 3, 2020).

[21] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last visited September 3, 2020).

credit reports and accounts and to undertake additional safeguards such as requesting new credit cards, changing passwords, and enrolling in a credit monitoring service.

49. Since the Data Breach occurred, Plaintiff has received multiple notices of someone attempting to log into his various accounts from locations outside of the United States. As a result, Plaintiff has spent and continues to spend his valuable time to protect the integrity of his personal information, finances, and credit—time which he would not have had to expend but for the Data Breach.

50. Plaintiff and Class Members have suffered actual injuries from having their PII and PHI exposed as a result of the Data Breach, including, but not limited to: (a) damages resulting from taking the time to search for fraudulent activity; to enroll in credit monitoring and identity theft protection; to call his creditors to provide them with notice of the breach; and to otherwise attempt to protect their financial accounts; (b) damages to and diminution in the value of his PII and PHI – a form of intangible property that he entrusted to OMSA as a condition of the provision of services to patients; and (c) imminent and impending injury arising from the increased risk of fraud and identity theft.

51. As a result of the Data Breach, Plaintiff and Class Members will continue to be at heightened risk for financial fraud, medical fraud, identity theft, and attendant damages for years to come.

52. The Data Breach was a direct and proximate result of OMSA's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII and PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII and

PHI; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

53. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately invest in data security measures, despite its obligations to protect PII and PHI. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of PII and PHI.

54. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[22]

55. To date, OMSA has offered inadequate identity monitoring services to affected individuals given the type of data stolen. They are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII

[22] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited September 3, 2020).

and PHI.

56. As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII and PHI;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII and PHI in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

57. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their PII and PHI are secure, remain secure, and are not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

58. Plaintiff seeks relief on behalf of himself and as representatives of all others who are similarly situated. Pursuant to Rules 23(a)(1)-(4) Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons whose PII and PHI was compromised as a result of the Data Breach announced by OMSA beginning on or about February 21, 2020 (the "Class").

59. Excluded from the Class are OMSA and any of its affiliates, parents or subsidiaries or employees; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

60. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

61. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

62. **Numerosity. Rule 23(a)(1), SCRCP.** Consistent with Rule 23(a)(1), the members of the Class are so numerous that the joinder of all members is impractical. The Data Breach implicates approximately more than 35,000 OMSA patients.

63. **Commonality. Rule 23(a)(2), SCRCP.** Consistent with Rule 23(a)(2), this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether OMSA had a duty to protect its patients' sensitive PII and PHI;

b. Whether OMSA knew or should have known of the susceptibility of its systems to a data breach;

c. Whether OMSA's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether OMSA was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether OMSA's failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether OMSA's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII and PHI;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of OMSA's failure to reasonably protect its systems and data network; and,

h. Whether Plaintiff and Class members are entitled to relief.

64. **Typicality. Rule 23(a)(3), SCRCP.** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class Members. Plaintiff is a patient of OMSA, as are all the other victims impacted by the breach. Plaintiff's damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief sought by the Class.

65. **Adequacy. Rule 23(a)(4). SCRC{.** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because he is a member of the Class he seeks to represent; is committed to pursuing this matter against OMSA to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff's attorneys are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

66. **Superiority.** This class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be

encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against OMSA, and thus, individual litigation to redress OMSA's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

67. **Injunctive and Declaratory Relief.** Class certification is also appropriate under via a class action. Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

68. Likewise, the issues within this case are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether OMSA owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII and PHI;

b. Whether OMSA's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

c. Whether OMSA's failure to institute adequate protective security measures amounted to negligence;

d. Whether OMSA failed to take commercially reasonable steps to safeguard patients' PII and PHI;

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach; and

f. Whether OMSA failed to comply with its statutory and regulatory obligations.

69. Finally, all members of the proposed Class are readily ascertainable. OMSA has access to its patients' names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing notice.

FIRST CAUSE OF ACTION
NEGLIGENCE

70. Plaintiff restates, realleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

71. As a condition of receiving treatment with OMSA, Plaintiff and Class Members were obligated to provide OMSA with their PII and PHI.

72. Plaintiff and the Class Members entrusted their PII and PHI to OMSA with the understanding that OMSA would safeguard their information.

73. Defendant had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and Class Members could and would suffer if that information were wrongfully disclosed.

74. Defendant had a duty to exercise reasonable care in safeguarding, securing and

protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing the Defendant's security protocols to ensure that individuals' PII and PHI in OMSA's possession was adequately secured and protected and that employees tasked with maintaining such information were adequately trained on cybersecurity measures regarding the security of such information.

75. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing PII and PHI of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyberscams being perpetrated, and that it had inadequate employee training and education and IT security protocols in place to secure the PII and PHI of Plaintiff and the Class.

76. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII and PHI of Plaintiff and Class Members.

77. In addition, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as OMSA, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

78. OMSA violated Section 5 of the FTC Act by failing to use reasonable measures to

protect patients' PII and PHI and not complying with applicable industry standards, as described in detail herein. OMSA's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

79. Plaintiff and the Class Members had no ability to protect their PII and PHI that was in OMSA's possession.

80. Defendant was able to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

81. Defendant had a duty to put proper procedures in place in order to prevent the unauthorized dissemination of Plaintiff's and Class Members' PII and PHI.

82. Defendant admitted that Plaintiff's and Class Members' PII and PHI was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

83. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the Plaintiff's and Class Members' PII and PHI while it was within the OMSA's possession or control.

84. Defendant improperly and inadequately safeguarded Plaintiff's and Class Members' PII and PHI in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

85. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII and PHI.

86. Defendant, through its actions and/or omissions, unlawfully breached its duty to

timely and adequately disclose to Plaintiff and Class Members the existence, and scope of the Data Breach.

87. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII and PHI would not have been compromised.

88. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and PHI and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

89. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

90. Plaintiff restates, realleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

91. Plaintiff and Class Members were required to provide their PII and PHI, including their names, Social Security Numbers, addresses, medical record numbers, dates of birth, telephone numbers, email addresses, and various other sensitive information to Defendant as a condition of receiving treatment with OMSA.

92. In its written privacy policies provided to patients on their first visit to OMSA, OMSA promised Plaintiff and Class Members that it would only disclose PII and PHI under certain circumstances to authorized third parties, none of which relate to the Data Breach.

93. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII and PHI, was the latter's obligation to: (a) use such information for business purposes only; (b) take reasonable steps to safeguard that information; (c) prevent unauthorized disclosures of both PII and PHI; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and PHI; (e) reasonably safeguard and protect the PII and PHI of Plaintiff and Class Members from unauthorized disclosure or uses; and (f) retain the PII and PHI only as long as necessary and under conditions that kept such information secure and confidential.

94. Without such implied contracts, Plaintiff and Class Members would not have provided their PII and PHI to Defendant until such time that Defendant could properly safeguard that information. In addition, Plaintiff and Class Members would not have proceeded with their treatments at OMSA until such time as OMSA could guarantee that their PII and PHI would be adequately secured and protected against disclosure.

95. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

96. Defendant breached the implied contracts with Plaintiff and Class Members by failing to, *inter alia*:

a. Reasonably safeguard and protect Plaintiff's and Class Members' PII and PHI, which was compromised as a result of the Data Breach;

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

c. Implement technical policies and procedures for electronic information

systems that maintain electronic PII and PHI 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);

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

e. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii); and

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

97. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

THIRD CAUSE OF ACTION
VIOLATION OF CONSUMER IDENTITY THEFT PROTECTION ACT
S.C. Code Ann. § 39-1-90, *et seq.*

98. Plaintiff restates and realleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

99. Defendants' employees and agents, at all relevant times, acted within the course and scope of their employment by Defendant.

100. Defendant is vicariously liable for the actions and omissions of its employees and agents.

101. Plaintiff and Class Members possess and enjoy legal rights pursuant to the Consumer Identity Theft Protection provisions contained in the South Carolina Consumer Protection Code, S.C. Code Ann.§ 37-20-110 et seq.

102. Defendant is a "person" or "organization" as defined in the Consumer Protection Code. S.C. Code Ann. § 37-20-110(10) and§ 37-1-301(18) and (20).

103. Defendant possessed and required Plaintiff and Class Members to submit "personal identifying information" as a condition of receiving healthcare treatment. S.C. Code Ann.§ 37-20-110(1 l)(a) and§ 16-3-510(D).

104. A "security breach" occurred as a result of Defendant's knowing, willful, negligent or wrongful actions or omissions, as described herein. S.C. Code Ann.§ 37-20-110(15).

105. As a result of Defendant's knowing, willful or negligent violations, the personal identifying information of Plaintiff and Class Members was not adequately protected from theft by unauthorized persons or use for improper or unlawful purposes, and now or in the future may be publicly posted or displayed in violation of the law. S.C. Code Ann.§§ 37-20-110(13) and 37-20-180.

106. As a result of Defendant's knowing or willful violations, Plaintiff and Class Members each are entitled to recover three times the amount of actual damages or three thousand dollars for each incident, whichever is greater, as well as reasonable attorney's fees and costs. S.C. Code Ann.§ 37-20-170(D).

107. As a result of Defendant's negligent violations, Plaintiff and Class Members each are entitled to recover the greater of actual damages or one thousand dollars for each incident, as

well as reasonable attorney's fees and costs. S.C. Code Ann. § 37-20-170(E).

108. As a result of Defendant's breach of these statutes and failure to timely and properly notify its patients about the security breach in February 2020, Plaintiff and Class Members in South Carolina were deprived of the ability for some four months to take actions to protect their identity, including, but not limited to, placing a fraud alert on their credit reporting accounts, placing a security freeze on their credit reporting accounts, more closely monitoring their credit reporting accounts, or taking other actions to protect their identity, personal, private information and livelihood.

109. As a direct and proximate result of Defendant's actions, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

110. Plaintiff and Class Members are entitled to recover actual, special and consequential damages from Defendant in an amount to be determined by a jury of their peers.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT

111. Plaintiff restates and realleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

112. Plaintiff and Class Members conferred a benefit on Defendant by agreeing to work for OMSA and to further OMSA's financial interest and performance. Specifically, by becoming patients of OMSA, the Plaintiff, Class Members and their insurers paid OMSA for consultations and surgical procedures. In exchange, Plaintiff and Class Members should have received the

benefit of OMSA's commitments to safeguard PII with adequate data security.

113. Further, Defendant enriched itself by the savings on expenses related to data security measures to safeguard the PII and PHI in its possession. In lieu of providing a reasonable an adequate level of security for its industry, Defendant saved money and increased profits by utilizing ineffective, and somewhat cheaper, security measures.

114. Defendant knew that Plaintiff and Class Members conferred benefits which Defendant accepted. Defendant thus profited from these transactions and used the PII and PHI of Plaintiff and Class Members to further its business purposes.

115. The amounts OMSA received on behalf of the work completed by its patients were used, in part, to pay for use of OMSA's network and the administrative costs of data management and security.

116. Under the principles of equity and good conscience, Defendant should not be permitted to reap such benefits because Defendant failed to implement appropriate data management and security measures.

117. Defendant acquired the Plaintiff's and Class Members' PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

118. Plaintiff and Class Members have no adequate remedy at law.

119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI are used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and

attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

120. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

121. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FIFTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF

122. Plaintiff restates and reallege paragraphs all preceding paragraphs as if fully set forth herein.

123. Plaintiff seeks a declaration that: (i) OMSA's existing data security measures do not comply with its contractual obligations and duties of care; and (ii) in order to comply with its contractual obligations and duties of care, OMSA must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on OMSA's systems on a periodic basis, and

ordering OMSA to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing and training its security personnel regarding any new or modified procedures;

d. Segmenting customer data by, among other things, creating firewalls and access controls so that if one area of OMSA is compromised, hackers cannot gain access to other portions of OMSA's systems;

e. Purging, deleting and destroying PII and PHI not necessary for its provisions of services in a reasonably secure manner;

f. Conducting regular database scans and security checks;

g. Routinely and continually conducting 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

h. Educating its patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps patients should take to protect themselves.

124. As a direct result of OMSA's knowing violations of HIPAA, the FTCA and industry standards, Class Members are entitled to a declaration that: (i) OMSA's existing data security measures do not comply with the requirements imposed upon it by law; and (ii) in order to comply with its legal obligations and duties of care, OMSA must implement and maintain reasonable security measures, including but not limited to, injunctive relief:

a. Ordering that OMSA 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 on a periodic basis, and ordering OMSA to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that OMSA engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that OMSA audit, test and train its security personnel regarding any new or modified procedures;

d. Ordering that OMSA segment PII and PHI by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of OMSA's systems;

e. Ordering that OMSA purge, delete and destroy PII and PHI not necessary for its provisions of services in a reasonably secure manner;

f. Ordering that OMSA conduct regular database scans and security checks;

g. Ordering that OMSA routinely and continually 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

h. Ordering OMSA to meaningfully educate its patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as steps OMSA patients should take to protect themselves.

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, respectfully request the following relief:

i. An Order certifying this case as a class action;

j. An Order appointing Plaintiff as the class representative;

k. An Order appointing undersigned counsel as class counsel;

l. An Order compelling Defendant to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received;

m. A mandatory injunction directing the Defendant to hereinafter adequately safeguard the PII and PHI of Plaintiff and the Class by implementing improved security procedures and measures;

n. An award of damages;

o. An award of costs and expenses;

p. An award of attorneys' fees; and

q. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demand a jury trial as to all issues triable by a jury.

Respectfully submitted,

MORGAN & MORGAN

/s/ Patrick Graves, Esq.
Patrick Graves
170 Meeting Street
Suite 110
Charleston, SC 29401
Telephone: (843) 973-5180
Email: pgraves@forthepeople.com

John A. Yanchunis*
Patrick A. Barthle*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
jyanchunis@forthepeople.com
pbarthle@forthepeople.com

Joel R. Rhine*
Martin A. Ramey*
RHINE LAW FIRM, P.C.
1612 Military Cutoff Rd., Suite 300
Wilmington, NC 28403
Telephone: (910) 772-9960
jrr@rhinelawfirm.com
mjr@rhinelawfirm.com

Counsel for Plaintiff and the Putative Class

*Motions for *pro hac vice* admission to be filed

EXHIBIT A

ORAL AND MAXILLOFACIAL SURGERY ASSOCIATES, PA

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]
SHAWN A PETICOS
[redacted]

June 17, 2020

Dear Shawn A Peticos,

What Happened

We are writing to notify you that Oral and Maxillofacial Surgery Associates, P.A. (the "Practice") was victimized by a cyberattack (the "Incident"). We immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope, the impact on our information systems, and the identities of those the Incident may have affected.

On or about April 22, 2020, we determined that, on February 21, 2020, the cyberattacker may have accessed files on our systems that contain personal health information ("PHI") and/or personally identifiable information ("PII") that relates to you. We have not found any evidence that the information contained in the affected files was misused as a result of the Incident.

What Information Was Involved

The files potentially accessed as a result of the Incident contained one or multiple data elements of PHI and/or PII including names, X-ray and other treatment-related images, and/or dates of birth.

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we have arranged for TransUnion to provide to you 12 months of free credit monitoring and related services. Please see the attached instructions on how to enroll. To receive these services, please be sure to enroll by **September 30, 2020**. Your activation code is: [redacted]

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since learning of the attack, we have taken a number of steps to further secure our systems. Specifically, we have, among other things: formatted our server and all impacted workstations; vetted and monitored all equipment attached to our network; and replaced operating systems and workstations that were compromised as a result of the Incident.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

If you have questions or concerns, please contact 855-917-3551 Monday through Friday 9am to 9pm Eastern Time. We sincerely apologize for this situation and any inconvenience it may cause you.