



David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, New York 11201
dmcmillan@constangy.com
Direct: 718.614.8371

March 28, 2024

Via E-MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Tel: 410-576-6491

Email: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Northern Virginia Oral, Maxillofacial & Implant Surgery (“NOVA OMS”) in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On October 5, 2023, NOVA OMS became aware of unusual activity on its network. In response, NOVA OMS took immediate steps to secure its digital environment and engaged a leading cybersecurity firm to conduct an investigation to determine whether any personal or protected health information may have been accessed or acquired during the incident. Based on that investigation, NOVA OMS learned that an unknown criminal actor gained unauthorized access to its network between October 3 – 6, 2023 and accessed or acquired certain files, some of which contained individuals’ personal or protected health information. NOVA OMS undertook a comprehensive review of the impacted data to determine what may have been affected and the individuals involved. On February 28, 2024, NOVA OMS confirmed that personal information belonging to certain Maryland residents may have been involved. NOVA OMS then took steps to notify those individuals as quickly as possible.

NOVA OMS is notifying all potentially impacted individuals of this incident, providing them with steps they can take to protect their personal information, and offering free credit and identity monitoring services to individuals whose Social Security or individual tax identification numbers may have been impacted.

Please note that we have no current evidence to suggest misuse or attempted misuse of any personal information in conjunction with this incident.

2. Number of Maryland residents affected.

NOVA OMS notified 597 Maryland residents of this incident via first class U.S. mail on March 28, 2024. The information potentially impacted in connection with this incident varies by individual, but may include name, date of birth, medical information, health insurance information, driver's license or state identification card information, individual tax identification number, patient ID, and Social Security number.

A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as NOVA OMS discovered this incident, NOVA OMS took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal and protected health information potentially impacted. In addition, NOVA OMS implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future. NOVA OMS also notified the Federal Bureau of Investigation.

NOVA OMS has established a toll-free call center through Epiq, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while NOVA OMS is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, NOVA OMS is also providing complimentary credit and identity protection services to notified individuals whose Social Security or individual tax identification numbers may have been impacted.

4. Contact information.

NOVA OMS remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

/s/ David McMillan

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<First Name>> << Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

To Enroll, Please Call:
1-877-288-8057
Or Visit:
<https://www.experianidworks.com/3bcredit>
Enrollment Code: <<Activation Code>>
Engagement Number: <<Engagement #>>

<<Date>>

Subject: Notice of Data <<Breach/Incident>>

Dear <<First Name>> << Last Name>>:

Northern Virginia Oral, Maxillofacial & Implant Surgery (“NOVA OMS”) is writing to inform you of a recent data security incident that may have involved your personal information and / or protected health information. NOVA OMS takes the privacy and security of all information within its possession very seriously. We are writing to notify you about the incident, provide you with information about steps you can take to help protect your information, and offer you the opportunity to enroll in complimentary identity protection services that NOVA OMS is making available to you.

What Happened? On October 5, 2023, NOVA OMS discovered unusual activity in its network environment. Upon discovering this activity, NOVA OMS immediately took steps to secure its network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. The investigation subsequently revealed that certain personal information and / or protected health information may have been accessed or acquired without authorization between October 3, 2023 to October 6, 2023. On or about February 28, 2024, we completed a comprehensive review of the impacted data and identified your information as potentially involved. We then took steps to notify you of the incident as quickly as possible.

What Information Was Involved? The information that may have been impacted includes your name, driver’s license number, medical information, health insurance information, <<Breached Elements>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. In addition, we reported this incident to law enforcement and will cooperate as necessary. We also implemented additional security measures to help reduce the risk of a similar incident occurring in the future.

In addition, out of an abundance of caution, we are offering you complimentary identity protection services through Experian – a data breach and recovery services expert. These services include <<12/24>> months of credit monitoring¹, \$1 million identity theft insurance, and identity restoration services. Please note that the deadline to enroll in these services is <<Enrollment Deadline>>.

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What Can You Do? NOVA OMS recommends that you review the guidance included with this letter about how to protect your information. You can also enroll in the complimentary identity protection services being offered to you by using the Enrollment Code provided above.

For More Information: Further information about how to help protect your information appears on the following page. If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, please call Epiq at 1-866-264-1051 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays).

We take your trust in us and this matter very seriously. We regret any inconvenience that this may cause you.

Sincerely,

Northern Virginia Oral, Maxillofacial & Implant Surgery

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.