



Maria Efaplatidis, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, New York 11201
mefaplatidis@constangy.com
Mobile: 917.414.8991

March 31, 2023

VIA EMAIL: ldtheft@oag.state.md.us

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents OrthoAlaska, LLC ("OrthoAlaska"), a healthcare provider headquartered in Anchorage, Alaska, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute, Md. Code Ann. Comm. Law §§ 14-3501 - 3508.

1. Nature of the Security Incident

On March 3, 2023, OrthoAlaska learned that some personal information of its former employees may have been impacted by a security incident. On October 12, 2022 OrthoAlaska detected unusual activity in its systems. In response, OrthoAlaska immediately took steps to terminate the activity and to secure its network, systems, and data. It also retained independent cybersecurity experts to conduct a forensic investigation into the incident and determine what happened. The investigation indicated that an unauthorized party gained access to files stored within OrthoAlaska systems that contain information about its former employees. OrthoAlaska, with the assistance of outside data privacy and cybersecurity experts, conducted a thorough investigation to identify the individuals whose personal information may have been impacted by this incident and the categories of information potentially involved for each individual. After, OrthoAlaska worked to identify current contact information to notify potentially impacted individuals of what happened.

To date, OrthoAlaska has no reason to believe that personal information of potentially impacted individuals has been misused as a result of this incident. Out of an abundance of caution, OrthoAlaska is notifying all potentially impacted individuals of the incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for approximately 3 Maryland residents. The information involved in the incident may differ depending on the individual but may include the following for affected Maryland residents: name in combination with Social Security number. Again, OrthoAlaska has no reason to believe that the information involved has been or will be published, shared, or otherwise misused.

3. Notification to Affected Individuals

On April 3, 2023, notification letters will be sent to affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services to each individual whose Social Security numbers was affected by this event, including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Those services are offered through Experian. Experian will also support a call center for 90 days to answer questions and assist with enrollment. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

In response to the incident, OrthoAlaska retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. OrthoAlaska has implemented additional security measures to further harden its email tenant in an effort to prevent a similar event from occurring in the future.

Finally, OrthoAlaska is notifying the potentially affected individuals and providing them with steps they can take to protect their personal information as discussed above and reporting the incident to nationwide consumer reporting agencies (i.e., Equifax, Experian, and Transunion).

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at MEfaplatidis@constangy.com or 917.414.8991.

Sincerely,



Maria Efaplatidis of
Constangy, Brooks, Smith & Prophete LLP

ME:mff

Encl.: Sample Notification Letter

cc: Michael F. Ferragamo, Constangy (MFerragamo@constangy.com)



Return to IDX
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 3, 2023

Notice of Data Security << VAR DATA 2>>

Dear <<First Name>> <<Last Name>>,

We are notifying you of an incident that may have involved your personal information. OrthoAlaska, LLC (“OrthoAlaska”) takes the privacy and security of your information very seriously, which is why we are informing you of the incident and providing you with steps you can take to protect your information.

What happened? On March 3, 2023 we learned that some of your information may have been impacted by a security incident. On October 12, 2022, we discovered unauthorized activity on our systems. In response, we immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure our network, systems, and data. In addition, we retained independent cybersecurity experts to conduct a forensic investigation into the incident and assist us in determining what happened. This forensic investigation determined that there was unauthorized access to files stored within our systems that contain information about our former employees.

With the assistance of outside data privacy and cybersecurity experts, OrthoAlaska conducted a thorough investigation to identify the individuals whose personal information may have been impacted by this incident and the categories of information potentially involved for each individual. That investigation determined that the impacted systems contained some of your personal information. Please note that we have no reason to believe that your information was published, shared, or misused as a result of this incident. Nevertheless, out of an abundance of caution, we are notifying you to provide you with steps that you can take to protect your information.

What Information Was Involved? The information potentially involved included <<VAR DATA 1>>.

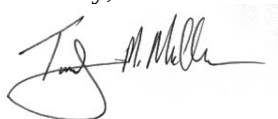
What We Are Doing: As soon as we discovered the incident, we took the steps described above, including performing a thorough review of our systems to investigate the incident and ensure that our systems remain secure, and implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents. We also reported the incident to the Federal Bureau of Investigation and will cooperate to help identify and prosecute those responsible.

Additionally, we are offering you complimentary identity theft protection services through IDX. These services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling **1-800-939-4170** or going to [**https://app.idx.us/account-creation/protect**](https://app.idx.us/account-creation/protect) and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 5:00 am – 5:00 pm Alaska Time. Please note the deadline to enroll is July 3, 2023. Again, there is no evidence that your information has been misused. However, we encourage you to take advantage of this offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information: If you have any questions about this letter, please contact us at **1-800-939-4170**. IDX representatives are available Monday through Friday from 5:00 am – 5:00 pm Alaska Time. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Tim Mullen", with a large, stylized initial "T" and "M".

Timothy M. Mullen
Chief Executive Officer
OrthoAlaska, LLC

Steps You Can Take to Protect Your Personal 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 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
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
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th 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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.