



Lauren Godfrey, Esq.
322 North Shore Drive
Building 1B, Suite 200
Pittsburgh, Pennsylvania 15212
lgodfrey@constangy.com
Tel: 412.870.4129

February 13, 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

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith and Prophete LLP (“Constangy”) represents Carr Maloney, P.C. in connection with an incident described in greater detail below.

1. Nature of Incident

On or about December 6, 2023, Carr Maloney discovered unusual activity in its email tenant. Upon discovering this activity, Carr Maloney immediately took steps to secure its email tenant and launched an investigation to determine what happened and whether sensitive information may have been affected. The investigation subsequently revealed that information contained in one employee’s email account may have been accessed or acquired without authorization during the incident. Carr Maloney then conducted a comprehensive review of the data contained in the email account. In January 2024, Carr Maloney completed that review and determined that certain personal information was contained in the account.

The potentially affected information varied by individual but may include the following: individuals’ names, Social Security numbers, driver’s license numbers, health insurance information, and medical information.

2. Number of Maryland residents affected

Carr Maloney notified thirty-nine (39) Maryland residents of the incident via first class U.S. mail on February 13, 2024. The impacted individuals were not employees. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the incident

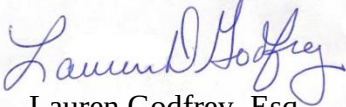
Upon discovering the issue, Carr Maloney took the steps described above. Carr Maloney also provided notice of the incident to potentially impacted individuals on February 13, 2024. In

addition, Carr Maloney is offering affected individuals, whose Social Security numbers were impacted, complimentary credit monitoring and identity protection services through IDX, a ZeroFox Company, the data breach and recovery services expert. These services include 12 months of credit monitoring, identity protection, and fully managed identity theft recovery services. With this protection, IDX will help impacted individuals resolve issues if their identity is affected.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at 412.870.4129 or lgodfrey@constangy.com.

Very truly yours,



Lauren Godfrey, Esq.

Encl.: Sample Consumer Notification Letter

Carr Maloney P.C.

Return to IDX:
4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

<<first name>> <<last name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

February 13, 2024

Subject: Notice of Data Security Incident

Dear <<first name>> <<last name>>:

I am writing to inform you of a data security incident that may have affected your personal information. At Carr Maloney, P.C., we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services.

What Happened. On or about December 6, 2023, Carr Maloney discovered unusual activity in its email tenant. Upon discovering this activity, Carr Maloney immediately took steps to secure its email tenant and launched an investigation to determine what happened and whether sensitive information may have been affected. The investigation subsequently revealed that information contained in one employee's email account may have been accessed or acquired without authorization during the incident. We then conducted a comprehensive review of the data contained in the email account. In January 2024, we completed that review and determined that your information was contained in the account. We then took steps to notify you of the incident as quickly as possible. We have no information that your personal information has been misused as a result of the incident.

What Information Was Involved. The information involved in this incident may have included your name and <<variable text2>>.

What We Are Doing. As soon as Carr Maloney discovered the incident, we took the steps described above. We also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

In addition, we are offering you complimentary credit monitoring and identity protection services through IDX, a leader in consumer identity protection. These services include <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered to you through IDX, A ZeroFox Company, by contacting IDX at 1-800-939-4170 or going to <https://app.idx.us/account-creation-protect> and using the enrollment code above. Please note the deadline to enroll is May 13, 2024.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-800-939-4170 Monday through Friday from 9:00 AM to 9:00 PM Eastern. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Carr Maloney, P.C.

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 740256
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian

P.O. Box 2002
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

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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.