



Jason S. Cherry, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East, Suite 1100
Los Angeles, CA 90067
jcherry@constangy.com
Mobile: 207.745.1397

March 1, 2023

VIA EMAIL: Idtheft@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 Heimerl & Lammers, LLC (“Heimerl & Lammers”) 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 February 6, 2023, Heimerl & Lammers learned that certain information of its current and former employees and contractors may have been impacted by a data security incident. On October 8, 2022, Heimerl & Lammers detected unusual activity in its systems. In response, Heimerl & Lammers 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 forensic investigation determined that there may have been unauthorized access to files stored within Heimerl & Lammers systems, including those that store personal information. Heimerl & Lammers then worked diligently to identify individuals whose information may have been impacted, as well as their current address information to notify all potentially impacted individuals about the incident. That review was completed on February 16, 2023.

To date, Heimerl & Lammers 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, Heimerl & Lammers 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 2 Maryland residents. The information involved in the incident may differ depending on the individual but may include the following for affected Maryland residents: Social Security number, Driver's License number, date of birth, and medical information if it was provided by the individual. Again, Heimerl & Lammers 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 March 1, 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. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

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

Finally, Heimerl & Lammers 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 JCherry@constangy.com or 201.745.1397.

Sincerely,



Jason S. Cherry of
Constangy, Brooks, Smith & Prophete LLP

JSC:mff

Encl.: Sample Notification Letter

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



Return Mail to: IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-753-4565
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

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

March 1, 2023

Notice of Data Security <<Variable 1>>

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

Heimerl & Lammers, LLC (“Heimerl & Lammers”) takes the privacy and security of your information very seriously. As such, we are informing you of a data security incident that may have involved your personal information. This notice explains the incident, provides you with steps you can take to protect your information, and offers you complimentary credit monitoring and identity protection services.

What happened? On February 6, 2023, our investigation of a data security incident determined that your personal information may have been affected by it. On October 8, 2022, we detected unusual activity in our systems. In response, we immediately shut down some systems and began an investigation with the help of third-party cybersecurity experts and incident response professionals. After a thorough investigation, it was determined that an outside party gained access to our computer systems. Because we take this incident seriously, we diligently worked to identify the individuals potentially impacted by this incident and their current mailing address information so that we could notify them about it. That review was completed on February 16, 2023. Please note that to date we have no reason to believe that your information has been misused as a result of this incident. Regardless, out of an abundance of caution, we are notifying you to provide you with steps you can take to protect your information.

What Information Was Involved? The data involved may have included your name in combination with a Social Security number, Driver’s License number, dates of birth, and medical information if you provided that to us.

What We Are Doing: In addition to the steps described above, we have worked with cybersecurity experts to enhance the security of our digital environment and prevent a similar incident from occurring in the future. We are also offering you complimentary identity theft protection services through IDX. These services include: <<12 / 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 1-833-753-4565 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is June 1, 2023. Again, at this time, 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: You will find detailed steps you can take to help protect your personal information on the following page. Also, 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 call 1-833-753-4565 or go to <https://app.idx.us/account-creation/protect> for help or for any questions you may have.

The privacy and security of your information is a top priority for Heimerl & Lammers, LLC. We take this incident very seriously and we regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in cursive script, appearing to read "Ben Heimerl", written in dark ink.

Benjamin J. Heimerl
Attorney
Heimerl & Lammers, 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

Minnesota Attorney General

445 Minnesota Street, Suite 1400
St. Paul, MN 55101
www.ag.state.mn.us
1-800-657-3787

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

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

North Carolina Attorney General

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

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.