



Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
aweaver@constangy.com
Mobile: 941.875.5335

March 27, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: Idtheft@oag.state.md.us

RE: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Campbell Killin Brittan & Ray, LLC ("Campbell Killin") in connection with a recent data security incident described below. Campbell Killin is notifying affected individuals of the incident. The purpose of this letter is to provide formal notice to your office pursuant to Md. Code Ann., Comm. Law § 14-3504.

I. Nature of the Security Incident

On July 17, 2023, Campbell Killin discovered unusual activity involving certain systems within its digital environment. Campbell Killin immediately took steps to secure its network. In addition, Campbell Killin retained an independent forensic investigator to assist in its response and conduct an investigation to determine what happened. That investigation revealed that an unauthorized actor gained access to the Campbell Killin network, and that some personal information may have been accessed or acquired without authorization in connection with the incident. Campbell Killin then commenced a comprehensive review of the potentially affected data to determine what information may have been involved, the individuals to whom the information pertained, and the addresses for those individuals. This process was completed on March 12, 2024. From this review, Campbell Killin identified that names, Social Security numbers, and/or medical information for Maryland residents may have been impacted. Campbell Killin thereafter worked diligently to arrange for notice and remediation services to the affected individuals.

II. Number of Maryland Residents Affected

Based on Campbell Killin's investigation, a total of thirty (30) Maryland residents may have been affected. Notification letters were sent to these individuals via first class U.S. mail on March 21, 2024. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

III. Actions Taken in Response to the Incident

As soon as Campbell Killin discovered the unusual network activity, it took immediate steps to secure its network, launched an investigation with the assistance of independent experts, and worked to determine whether any personal information was accessed or acquired without authorization in connection with the incident. Campbell Killin then worked diligently to determine what personal information may have been

affected, the individuals to whom the information pertained, and the addresses for those individuals to provide appropriate notification.

Campbell Killin has established a toll-free call center through IDX to answer questions about the incident and address related concerns. In addition, Campbell Killin is offering Maryland residents whose Social Security numbers may have been affected twelve (12) months of complimentary credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services through IDX.

IV. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 215.770.4234 or aweaver@constangy.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Aubrey L. Weaver', with a stylized, flowing script.

Aubrey L. Weaver
Partner, Cybersecurity & Data Privacy Team

Encl. Sample Consumer Notification Letter



C/O Return Mail Processing Center
P.O. Box 989728
West Sacramento, CA 95798-9728

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

March 21, 2024

Subject: Notice of Data <<Variable Data 1>>

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

Campbell Killin Brittan & Ray, LLC (“Campbell Killin”) is writing to inform you of a recent data security incident that may have affected your personal information. Campbell Killin takes the privacy and security of the information in its possession very seriously. That is why we are informing you of the incident and providing you with steps you can take to protect your information.

What Happened? On July 17, 2023, Campbell Killin experienced a disruption in our computer network. We immediately initiated an investigation and engaged digital forensics experts to assist us with the process. The forensic investigation determined that certain Campbell Killin data may have been acquired without authorization during the incident in July 2023. Campbell Killin thereafter undertook a comprehensive review of the affected data with the assistance of leading external experts to identify any personal information that may have been involved, the individuals to whom the information pertained, and the addresses for those individuals. This process was completed on March 12, 2024, at which time we determined that your information may have been involved and arranged to provide you this notification.

What Information Was Involved? The information may have included your <<Variable Data 2>>.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. We also notified the FBI and will provide whatever cooperation may be necessary to hold the perpetrators accountable. Campbell Killin has also implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future.

What You Can Do. You can follow the recommendations on the following page to help protect your information.

For More Information. Additional information about how to protect your information appears on the following page. If you have questions or need assistance, please call 1-888-685-6668 Monday through Friday from 7:00 am to 7:00 pm Mountain Time, excluding holidays.

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,

Campbell Killin Brittan & Ray, LLC

A handwritten signature in black ink, appearing to read "J. Kevin Ray", written over a horizontal line.

J. Kevin Ray, Managing Director
270 Saint Paul St, Suite 200
Denver, CO 80206

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://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.