



Donna Maddux, Partner
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, OR 97035
dmaddux@constangy.com
Direct: 503.312.6251

May 1, 2024

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Constangy, Brooks, Smith & Prophete, LLP represents Sequoia Climate Foundation (“Sequoia”), in conjunction with a recent data security incident described in greater detail below. Sequoia is a climate change foundation headquartered in Irvine, California. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification law.

1. Nature of the Security Incident

On or about October 2023, Sequoia discovered that two (2) former employees copied and retained certain data without authorization prior to departing the organization in August of 2023. Sequoia immediately initiated an investigation with the assistance of independent data security experts to determine what files were involved. Sequoia then engaged additional experts to conduct a thorough review of the files to determine what information may have been involved. On April 26, 2024, this investigation confirmed that the personal information of two (2) Maryland residents was involved.

Sequoia has no reason to believe this information has been misused.

2. Type of Information and Number of Maryland Residents Affected

Sequoia is notifying two (2) residents of Maryland of this data security incident via first class U.S. mail on May 2, 2024. The information accessed and potentially acquired by the former employee responsible for this incident may have included name, Social Security number, and health insurance

information. A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Sequoia implemented additional security features in an effort to prevent a similar incident from occurring in the future. Further, Sequoia has offered all individuals whose information was involved 12 months of complimentary services through IDX, which includes credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, fully-managed identity theft recovery services, and 90 days access to a call center. Finally, Sequoia worked to confirm the data was returned and/or deleted by the former employees.

4. Contact Information

Sequoia remains dedicated to protecting the personal information in its possession. Should you have any questions or need additional information, please do not hesitate to contact me at 503.312.6251 or by e-mail at dmaddux@constangy.com.

Best regards,

/s/ Donna Maddux

Donna Maddux
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter



Secure Processing Center
P.O. Box 2623
Duluth, GA 30096-9998

<<FirstName>> <<LastName>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Subject: Notice of Data <<Variable Header>>

Dear <<FirstName>> <<LastName>>:

The Sequoia Climate Foundation (“Sequoia”) is writing to inform you of a recent data security incident that affected your personal information. Sequoia takes the privacy and security of the information in its possession very seriously. That is why we are informing you of the incident, providing you with steps you can take to protect your information, and providing you with the opportunity to enroll in credit monitoring and identity protection services at no cost to you.

What Happened? In October of 2023, Sequoia discovered that two (2) former employees had copied and retained certain data without authorization prior to departing the organization. Sequoia immediately initiated an investigation with the assistance of independent data security experts to determine what files were involved. Sequoia then engaged additional experts to conduct a thorough review of the files to determine what information may have been involved. This process was completed on <<NCOA Date>>, 2024.

What Information Was Involved? The information included your name and your <<Breached Elements>>.

What We Are Doing. As soon as we discovered this incident, we took the steps described above, and have worked to confirm the data was returned and/or deleted by the former employees. The individuals who retained documents without authorization are no longer employed by Sequoia and they have no continuing access to Sequoia information systems or data.

In addition, although we have no reason to believe your information has been misused, we are offering you the opportunity to enroll in credit monitoring and identity theft protection services through Equifax. These services include 12 months of triple-bureau credit and WebScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your information. To enroll in the credit monitoring and identity protection services offered at no charge to you, please log on to www.equifax.com/activate, enter your unique Activation Code of <<Activation Code>>, then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

In order to receive the monitoring services described above, you must enroll by <<**Enrollment Deadline**>>.

For More Information. Additional information about how to protect your information appears on the following page. If you have questions or need additional assistance, please call 888-988-0342 Monday through Friday 6:00 am to 6:00 pm Pacific Time.

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,



James Jenkin, Chief Operating Officer
Sequoia Climate Foundation
2 Witherspoon
Irvine, CA 92604

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Additional information:

California: The California Attorney General can be reached at: 1300 “I” Street, Sacramento, CA 95814-2919; 1-800-952-5225; <http://oag.ca.gov/>.

Colorado: The Colorado Attorney General can be reached at: 1300 Broadway, 10th Floor, Denver, CO 80203; 1-720-508-6000; <https://coag.gov/>.

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us; <https://www.marylandattorneygeneral.gov/>.

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 1-877-5-NO-SCAM (Toll-free within North Carolina); 1-919-716-6000; <https://ncdoj.gov/>.