



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

November 8, 2023

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Maryland Attorney General's Office
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 ("Constangy"), represents Blue Ridge Electric Membership Corporation ("Blue Ridge Energy"), an energy cooperative in North Carolina, in connection with a recent third-party data security incident described in greater detail below. This notice is being provided because personal information for Maryland residents may have been involved in the incident.

1. Nature of the Security Incident

On September 27, 2023, Blue Ridge Energy was alerted of a data security incident that impacted the systems of Meridian, a vendor to Blue Ridge Energy. Through Blue Ridge Energy's independent monitoring of the situation, it learned that information belonging to Meridian had been released to the dark web in connection with the incident on October 12, 2023. Blue Ridge Energy thereafter conducted a thorough review of this data and identified that personal information for certain employees and members was involved. Blue Ridge Energy sent preliminary notification to these individuals via e-mail.

The potentially affected personal information for Maryland residents includes name and Social Security number.

2. Number of Maryland Residents Involved

On November 6, 2023, Blue Ridge Energy provided notification to 1 Maryland residents whose personal information may have been involved in this incident via first-class U.S. Mail. A sample copy of the notification is included with this correspondence.

3. Steps Taken to Address the Incident

As soon as Blue Ridge Energy was informed of the incident, it contacted Meridian for additional information, conducted its own monitoring of the situation, and comprehensively reviewed the

potentially affected data. Blue Ridge Energy is continuing to work with Meridian to better understand what happened and the potential impact to individuals' personal information.

Blue Ridge Energy has established a toll-free call center through TransUnion to answer questions about the incident and address related concerns. In addition, Blue Ridge Energy is offering twelve (12) months of complimentary credit and identity monitoring services to the potentially affected individuals.

4. Contact Information

Blue Ridge Energy remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at aweaver@constangy.com.

Sincerely,

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

Aubrey Weaver
Partner

Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter

Blue Ridge Energy
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB08068



[REDACTED]
address
City, MD Zip

November 6, 2023

Subject: Notice of Data Security Incident

Dear [REDACTED]:

We are writing to inform you of a recent third-party data security incident experienced by Meridian, a vendor to Blue Ridge Energy, that involved your personal information. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What happened?

On September 27, 2023, Blue Ridge Energy was alerted of a data security incident that impacted Meridian's systems. Through our independent monitoring of the situation, we learned that information belonging to Meridian had been released to the dark web in connection with the incident on October 12, 2023. We conducted a thorough review of this data and identified that personal information related to certain current and former employees was involved.

Please note that this incident did not impact Blue Ridge Energy's information systems.

What information was involved?

Based on our review, the information involved in this incident includes your name and Social Security number.

What are we doing?

As soon as we were made aware of the incident, we took steps to independently review the potentially affected information and provide notice in the most expedient time possible. We are continuing to meet regularly and work with key advisors, and Meridian, to better understand what happened and the potential impact to our employees and retirees. Although the risk of data breaches cannot be eliminated altogether, we are undertaking a thorough review to determine what more we can reasonably do to minimize risk going forward.

What can you do?

We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. If you notice suspicious activity in your financial records, you should report it immediately to your financial institution or issuing bank. Additional steps you can take to protect your personal information can be found on the enclosed sheet.

Additionally, we have arranged to provide you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in the Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/blueenergy> and follow the instructions provided. When prompted please provide the following unique code to receive services: **BHS3M9SBAX**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident and the protection of your personal information, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

Please be assured that Blue Ridge Energy takes the privacy and security of personal information very seriously. We hope you will accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Julie".

Julie O'Dell
SVP and Chief Administrative and Ethics Officer

Blue Ridge Energy
1216 Blowing Rock Blvd NE
PO Box 112 • Lenoir, NC 28645

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports, as detailed below. If you notice suspicious activity in your financial records, you should report it immediately to your financial institution or issuing bank.

Your data protection is important to us. We recommend you take these steps.

1. Freeze your credit with Equifax, Experian, and TransUnion. The links are provided below. We will also be posting those on Hello Blue.
2. If you don't already monitor your bank accounts on a regular basis, please take steps so you can monitor your accounts at least daily. Your bank can assist you in setting up your monitoring process based on your personal preferences.
3. If you have personal investment accounts, you may also want to contact them directly and ask what steps you need to take for fraud alerts.

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. Please be aware that placing a credit freeze may delay, interfere with, or prevent the timely approval of any requests you make for new loans, home mortgages, auto loans, employment, housing, or other services. 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.

You may also place a fraud alert on your credit report. A fraud alert is free and tells creditors to follow certain procedures like contacting you before they open any new accounts or change existing accounts. For example, when a creditor receives a request to change one of your existing accounts, before making the change that creditor may call you to verify that you requested a change to your existing account. You can place a fraud alert with one of the credit agencies listed below and that agency will alert the other two agencies.

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

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

You may also obtain a copy of your credit report, free of charge, whether you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report, once every 12 months from each of the agencies, by contacting any one of the following national consumer reporting agencies:

Experian:

www.experian.com or 1-888-397-3742 or P.O. Box 4500, Allen, TX 75013

TransUnion:

www.transunion.com or 1-800-680-7289 or Trans Union LLC, P.O. Box 1000, Chester, PA 19016

Equifax:

www.equifax.com or 1-800-525-6285 or Equifax Information Services LLC, P.O. Box 740241, Atlanta, GA 30374-0241

You can also order a free credit report by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf>) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.