

Clarity Telecom, LLC d/b/a Bluepeak
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024



May 7, 2026

Re: Notice of Security Incident

Dear [Redacted]:

Bluepeak¹ is writing to you about a recent incident that may have involved some of your personal information. We have taken steps to secure your information, and are not aware of any attempted or actual misuse of your personal information as a result of this incident. Nevertheless, we are providing this notice and information regarding the facts of this incident so you may take appropriate precautions, should you feel it is appropriate to do so.

What Happened? On the evening of December 11, 2025, we detected suspicious activity within the computer network at our Rapid City, South Dakota location. We promptly began an investigation, interrupted the attack, secured our systems, and notified law enforcement. As a result, there was no disruption to any of our services. We also hired several third parties to assist with our investigation and to ensure the security of our computer network. Unfortunately, we recently determined that some of the computer files copied off our systems contained your personal information.

What Information Was Involved? Upon review, we have determined the files may have involved your name, government identifier and/or information affiliated with our employee health insurance program.

What We Are Doing. In addition to the actions described above, we have taken steps to reinforce our computer network through the implementation of additional security measures. We will continue to make investments in cybersecurity to improve our resiliency.

What You Can Do. We have enclosed an *Identity Protection Reference Guide* to make you aware of ways to monitor and protect your personal information. We are also offering complimentary credit monitoring in case you find it helpful to review your credit report activity. For more information on credit monitoring services, including instructions on how to activate your complimentary two (2)-year membership, please see the additional information provided in this letter.

For More Information. If you have any questions or concerns, please reach out to our dedicated support team at [Redacted], Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern, excluding US holidays.

Sincerely,

Bluepeak

¹This notice is provided by Bluepeak, whose predecessors include Wow!, Vast Broadband, and Vexus Fiber.

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax

<https://www.equifax.com/personal/credit-report-services/>
1-888-298-0045
Equifax Fraud Alert, P.O. Box 105069
Atlanta, GA 30348-5069
Equifax Credit Freeze, P.O. Box 105788
Atlanta, GA 30348-5788

Experian

<https://www.experian.com/help/>
1-888-397-3742
Experian Fraud Alert, P.O. Box 9554,
Allen, TX 75013
Experian Credit Freeze, P.O. Box
9554, Allen, TX 75013

TransUnion

<https://www.transunion.com/credit-help>
1-800-916-8800
TransUnion Fraud Alert, P.O. Box 2000,
Chester, PA 19016
TransUnion Credit Freeze, P.O. Box
160, Woodlyn, PA 19094

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail,

the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze. There is no cost to place a security freeze.

4. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider.

5. You can also further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438- 4338); and TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

This notification was not delayed by law enforcement.

District of Columbia Residents: You can obtain additional information about identity theft prevention and protection from the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, <https://oag.dc.gov/>.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, <https://www.mass.gov/service-details/identity-theft>.

New Mexico Residents: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.

Rhode Island Residents: Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. The information of approximately 0 Rhode Island residents was involved in this incident.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

DETAILS REGARDING YOUR CYBERSCOUT MEMBERSHIP

We are offering you complimentary 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 two (2)-year 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, a TransUnion company specializing in fraud assistance and remediation services.

To activate your membership and start monitoring your credit, please follow the steps below:

- Ensure that you **enroll within 90 days from the date of this letter** (Your code will not work after this date.)
 - **Visit** the Cyberscout website to enroll: <https://bfs.cyberscout.com/activate>
 - Provide your **unique code:** [REDACTED]
- 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.**