



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

August 23, 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 ("Constangy"), represents ComNet Communications, Inc. ("ComNet"), a telecommunications company based in Connecticut, in connection with a recent 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 June 11, 2024, ComNet experienced an incident involving unauthorized access to certain network systems. When ComNet discovered this activity, ComNet immediately took steps to secure its systems and promptly launched an investigation. In so doing, ComNet engaged independent cybersecurity experts to conduct an investigation and to determine if personal information was impacted. As a result, on July 15, 2024, ComNet determined that certain ComNet employee data may have been accessed or acquired in the incident and took steps to gather contact information needed to provide notice to individuals whose information could have been involved.

The potentially affected personal information for Maryland residents includes names and Social Security numbers.

2. Number of Maryland Residents Involved

On August 23, 2024, ComNet provided notification to thirteen (13) 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

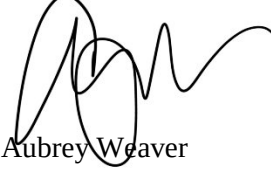
As soon as ComNet discovered this incident, it took the steps described above. In addition, ComNet has implemented several measures to enhance its security posture and reduce the risk of similar future incidents.

ComNet has also established a toll-free call center through IDX to answer questions about the incident and address related concerns. In addition, ComNet is offering 24 months of complimentary credit monitoring and identity protection services to the potentially affected individuals.

4. Contact Information

ComNet 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, flowing script.

Aubrey Weaver
Partner
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter



P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

August 23, 2024

Subject: Notice of Data <<Variable Text 2: Header>>

Dear <<First Name>> <<Last Name>>:

We are writing to notify you of a data security incident at ComNet Communications (“ComNet”) that may have impacted your personal information. ComNet takes the privacy and security of its employees’ personal information very seriously. That is why we are notifying you of the incident, providing you with steps you can take to help protect your information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On June 11, 2024, ComNet experienced an incident involving unauthorized access to certain network systems. When we discovered this activity, we immediately took steps to secure our systems and promptly launched an investigation. In so doing, we engaged independent cybersecurity experts to conduct an investigation and to determine if personal information was impacted. As a result, on July 15, 2024, we determined that certain ComNet data may have been accessed or acquired in the incident and took steps to gather contact information needed to provide notice to individuals whose information could have been involved.

What Information Was Involved? The personal information involved may have included your <<Variable Text 1: Data Elements>>.

What We Are Doing? As soon as ComNet discovered this incident, we took the steps described above. In addition, we have implemented several measures to enhance our security posture and reduce the risk of similar future incidents.

Additionally, ComNet is offering you the opportunity to enroll in complimentary credit monitoring and identity protection services for 24 months through IDX, a national leader in identity protection services. The IDX services, which are free to you upon enrollment, include a subscription for the following: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To enroll, please call 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> and provide the enrollment code at the top of this page. Please note you must enroll by November 23, 2024. 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.

What You Can Do. We encourage you to enroll in the credit protection services we are offering, which are at no cost to you. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: If you have questions or need assistance, please contact 1-800-939-4170 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Maintaining the security of employee personal information is one of our top priorities. We regret any concern or inconvenience that this may cause you.

Sincerely,

ComNet Communications

STEPS YOU CAN TAKE TO HELP 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 FTC 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 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 FTC 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:

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

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

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903 <http://www.riag.ri.gov> 1-401-274-4400

Washington D.C.: Washington D.C. Attorney General can be reached at: 400 S 6th Street, NW Washington, DC 20001 oag.dc.gov 1-202-727-3400