February 14, 2024

VIA EMAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General Peterson:

Constangy, Brooks, Smith & Prophete, LLP represents Superior Communications, Inc. ("Superior"), in conjunction with a recent data security incident described in greater detail below. Superior is a manufacturing and distribution company with their corporate office California and distribution centers in California and Tennessee. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification law.

1. Nature of the Security Incident

On July 12, 2023, Superior experienced a network disruption. Superior immediately took steps to secure its network environment and engaged cybersecurity experts to conduct an investigation to determine what happened. The investigation determined that certain files may have been acquired without authorization on or about July 9, 2023. Superior then engaged a third-party vendor to conduct a comprehensive review of the potentially affected data to determine whether personal information may have been involved. Superior then conducted a comprehensive review of the types of personal information involved and verified current mailing addresses for impacted individuals. On January 24, 2024, Superior confirmed that certain personal information may have been involved and worked diligently to notify these individuals.

2. Type of Information and Number of New Hampshire Residents Affected

Superior is notifying one (1) resident of New Hampshire of this data security incident via first class U.S. mail on February 14, 2024. The information accessed and potentially acquired by the unauthorized actor responsible for this incident may have included . A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Superior reported this incident to the Federal Bureau of Investigation's Internet Crime Complaint Center and will cooperate with any investigative efforts in an attempt to hold the perpetrator(s) of this incident responsible, if possible. Superior has also implemented additional security features in an effort to prevent a similar incident from occurring in the future. Further, Superior has offered all individuals whose information was involved 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.

4. Contact Information

Superior 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 or by e-mail at

Best regards,

/s/ Donna Maddux

Donna Maddux
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter

Return to IDX:
4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

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

February 14, 2024

Subject: Notice of Data <<Variable Text 1: Security Incident/Breach>>

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

Superior Communications, Inc. ("Superior Communications") is writing to inform you of a data security incident that may have involved your personal information. Superior Communications takes the privacy and security of personal information very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On July 12, 2023, Superior Communications experienced a network disruption. We immediately took steps to secure our network environment and engaged cybersecurity experts to conduct an investigation to determine what happened. The investigation determined that certain files may have been acquired without authorization on or about July 9, 2023. We then engaged a third-party vendor to conduct a comprehensive review of the potentially affected data to determine whether personal information may have been involved. We then conducted a comprehensive review of the types of personal information involved and verified current mailing addresses for impacted individuals. On January 24, 2024, we confirmed that some of your personal information may have been involved. Please note that we have no evidence of any actual or suspected misuse of information involved in this incident. Nonetheless, we are writing to inform you of the incident and to share steps you can take to protect your personal information.

What Information Was Involved? The information involved may include

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also implemented additional measures to reduce the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable. We are also offering you the ability to enroll in <<Variable Text 3: 12/24>> months of complimentary credit monitoring and identity protection services through IDX, A ZeroFox Company, a national leader in identity protection services. The IDX services, which are free to you upon enrollment, include a <<Variable Text 3: 12/24>>-month subscription for the following: credit monitoring, CyberScan dark web monitoring, fully managed identity recovery services, and $1 million in identity theft insurance coverage. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the IDX identity protection services, which are offered at no cost to you.

To enroll in the services provided through IDX, please scan the QR above, call 1-800-939-4170 Monday through Friday from 6:00 am – 6:00 pm Pacific Time, or visit https://app.idx.us/account-creation/protect and insert the Enrollment Code provided above. Please note the deadline to enroll in these complimentary services is May 14, 2024. To receive credit monitoring services, you must be over the age of 18 and have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Please do not discard this letter, as you will need the Enrollment Code provided above to access services.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call please call IDX at 1-800-939-4170. IDX representatives are available Monday through Friday from 6:00 am – 6:00 pm Pacific Time. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

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,

Jill Hackerd
Vice President, Human Resources
Superior Communications, Inc.

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 poof. 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:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; oag@dc.gov; https://oag.dc.gov/.

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

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 1-212-416-8433; https://ag.ny.gov/.

Rhode Island: The total number of individuals receiving notification of this incident is <<#>>. The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov.

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 1-800-621-0508; texasattorneygeneral.gov/consumer-protection/.

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 1-802-828-3171; ago.info@vermont.gov; https://ago.vermont.gov/.