Maria Efaplomatidis, Partner
Cybersecurity & Data Privacy Team
45 Main Street, Suite 206
Brooklyn, NY 11201
Mobile: 917.414.8991
Email: mefaplomatidis@constangy.com

May 8, 2026

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

RE: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents Verber Dental Group PC ("Verber Dental") in connection with a recent data security incident described below. This notice is being sent on behalf of Verber Dental because personal information for 2 New Hampshire residents could have been involved in the incident.

I. NATURE OF THE SECURITY INCIDENT

On January 27, 2026, Verber Dental was alerted to unusual activity within its network. In response, Verber Dental took measures to ensure its environment was secure. Verber Dental also initiated an investigation, which revealed that certain data may have been accessed or acquired without authorization between January 26, 2026 – January 27, 2026. Verber Dental thereafter undertook a comprehensive review of the potentially affected information and worked to gather information needed to provide notice. This process concluded on May 1, 2026.

The potentially affected information varies for each individual but may have included individuals' names, Social Security Number, and/or driver's license or state identification number.

II. NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

On May 7, 2026, Verber Dental notified 2 New Hampshire residents within the potentially affected population, via USPS First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

III. ACTIONS TAKEN IN RESPONSE TO THE INCIDENT

As soon as Verber Dental discovered the potential email issue, it took immediate steps to secure the affected email account, launched an investigation with the assistance of independent experts, and worked to determine whether any personal information was accessed or acquired without authorization in connection with the incident. Verber Dental thereafter worked diligently to determine what personal information may

have been affected, the individuals to whom the information pertained, and the addresses for those individuals to provide appropriate notification.

Verber Dental has established a toll-free call center through TransUnion to answer questions about the incident and address related concerns. In addition, Verber Dental is offering individuals residents whose Social Security numbers or driver's license information was involved twelve (12) months of complimentary credit and identity protection services through TransUnion.

Verber Dental is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Verber Dental is also providing individuals with information on how to place a fraud alert and security freeze on their credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

IV. CONTACT INFORMATION

If you have any questions or need additional information, please do not hesitate to contact me at 917.414.8991or mefaplomatidis@constangy.com.

Sincerely,

Maria Efaplomatidis
Partner, Cybersecurity & Data Privacy Team

Encl. Sample Consumer Notification Letter

0006919

Verber Dental Group PC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS3715

21_0006919

VERBER DENTAL GROUP

[redacted]

May 7, 2026

Subject: Notice of Data Security Incident

Dear [redacted],

I am writing to inform you of an incident that may have affected some of your personal information. Verber Dental Group PC ("Verber Dental") is committed to maintaining the privacy and security of all information in our possession. This letter includes information about the incident and provides you with steps you can take to protect your personal information, along with a complimentary offer of credit and identity monitoring services.

What happened? On January 27, 2026, we were alerted to suspicious activity in our network. In response, we immediately took measures to ensure our network was secure and initiated an investigation to determine the full nature and scope of the event. We also engaged cybersecurity experts to assist with this process. Our investigation determined that some information may have been viewed or acquired without authorization between January 26, 2026 – January 27, 2026. We then engaged a third party to conduct a comprehensive review of all potentially affected information. The review, which concluded in April 2026, determined that some of your personal information was contained in the potentially affected data. We then took steps to locate contact information needed to notify individuals. At the conclusion of this process on May 1, 2026, we arranged for notification to potentially affected individuals.

What Information Was Involved? The potentially affected information may have included your name and the following: [redacted]. We have no evidence of any actual or attempted misuse of this information.

What We Are Doing: As soon as we discovered the incident, we took the steps described above. We also performed a thorough review of our systems to investigate the incident and enhance our network security. We implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents.

Additionally, to help protect your information, we are offering 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 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, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do: Receiving this letter does not mean that you are the victim of identity theft. We recommend that you review the guidance included with this letter about how to protect your information. We also encourage you to enroll in the complimentary monitoring services being offered to you through TransUnion by using the enrollment information provided.

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted]. 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. Please note the deadline to enroll in these services is 90 days from the date of this letter.

For More Information: If you have any questions about this letter, please contact our dedicated call center for this incident at **1-833-289-3692**. Representatives are available Monday through Friday from 8:00 am – 8:00 pm Eastern Daylight Time, excluding holidays, and have been fully versed on this incident.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Verber Dental Group PC
50 Utley Drive,
Camp Hill, PA 17011

0006919

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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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 (the "FTC").

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 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
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 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file 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. 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. 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.

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.

Equifax
P.O. Box 105851
Atlanta, GA 30348
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 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.