Delta Dental of Virginia
c/o Cyberscout
[Return Address]
<City>, <State> <Zip>

To Enroll, Please Visit:
https://bfs.cyberscout.com/activate
Enrollment Code: <<UniqueCode>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address 2>>
<<City>>, <<State>> <<PostalCode+4>>

<<Date>>

Subject: Notice of Data <<Custom Field 1>>

Dear <<FirstName>> <<LastName>>:

I am writing to inform you about a recent data security incident that may have affected your personal information. Delta Dental of Virginia ("DDVA") takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On or around April 23, 2025, DDVA discovered suspicious activity associated with one email account and immediately initiated an investigation of the matter. DDVA engaged independent cybersecurity experts to assist with the process. As a result of the investigation, DDVA determined that certain emails and attachments may have been accessed and acquired without authorization between March 21, 2025 and April 23, 2025. DDVA undertook a comprehensive review of those files and upon completion of that review, learned that some of your personal information was contained within the potentially affected data. That is the reason for this notification. Please note that DDVA has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your <<Exposed Data Elements>>.

What We Are Doing. As soon as DDVA discovered this incident we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. DDVA is also offering you complimentary identity protection services through TransUnion, a leader in consumer identity protection. These services include <<Service Length>> of credit monitoring[1], dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is 90 days from the date on this letter.

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 complementary services offered to you through TransUnion by using the enrollment code provided above. Also, as a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely.

[1] To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 1-833-303-6496 Monday through Friday from 8 am to 8 pm Eastern Time. 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,

Delta Dental of Virginia
5415 Airport Road
Roanoke, VA 24012
1-800-237-6060

Steps You Can Take to Help Protect Your Personal 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 1000
Chester, PA 19016
1-800-916-8800
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 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. 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.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

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.