Cooley

Kris Kleiner
+1 720 566 4048
kkleiner@cooley.com

Via Certified Mail

April 16, 2019

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sir or Madam:

I write on behalf of my client, Delta Dental of Illinois ("DDIL"), to inform you of a potential security incident involving certain personal information, which may have affected approximately nine New Hampshire residents. DDIL operates as a not-for-profit Dental Service Plan Corporation as well as a business associate and third-party service provider to certain Illinois groups that offer dental and vision insurance services to employees and individuals. While we have no evidence indicating that any particular information has been or will be misused, out of an abundance of caution, DDIL is providing notice to potentially affected individuals and to your office on behalf of the groups listed in Appendix A.

DDIL recently learned that an individual appears to have gained unauthorized web-based access to an email account belonging to a DDIL employee. Based on a forensic investigation performed by an independent third-party, we discovered who the impacted members were on March 1, 2019. Although we still do not have evidence that the outside individual who accessed the email account actually viewed any of its contents, it appears that such individual had access to the email account between the dates of December 21 and December 28, 2018. Because the information maintained in the account included certain personal information, such as first and last name, date of birth, address, dental or vision insurance information and Social Security number, this information could be affected by this incident. Accordingly, and out of an abundance of caution, DDIL is providing notice to potentially affected individuals and to your office in the event that an unauthorized person was able to view any such information. Please note that this incident did not affect any of DDIL's internal network or systems.

DDIL takes the privacy of personal information seriously and deeply regrets that this incident occurred. Upon learning of the event, DDIL promptly took steps to address the situation, including initiating an internal investigation, disabling the affected user account, and retaining a top forensic investigator to assist in the investigation. DDIL is also implementing additional email security tools designed to help prevent this type of incident from reoccurring in the future. Finally, DDIL has contacted law enforcement and will cooperate in any further investigation of this incident.

Potentially affected individuals are being notified via written letter, which will begin mailing on or around April 16, 2019. A form copy of the notice being sent to the potentially affected New Hampshire residents is included for your reference. If you have any questions or need further information regarding this incident, please contact me at (720) 566-4058 or kkleiner@cooley.com.

Cooley

Sincerely,

Kristopher Kleiner

Enclosure

Cooley LLP 380 Interlocken Crescent Suite 900 Broomfield, CO 80021-8023
t: (720) 566-4000 f: (720) 566-4099 cooley.com

Cooley

Appendix A

Group	Address	Number of New Hampshire Residents
DELTA DENTAL OF ILLINOIS	111 Shuman Blvd., Naperville, IL 60563	2
MCDONALD'S LICENSEES HEALTH & WELFARE PLAN AND THE RONALD MCDONALD HOUSE CHARITIES HEALTH & WELFARE PLAN UNDER THE MCDONALDS LICENSEES AND RONALD MCDONALD HOUSE CHARITIES HEALTH & WELFARE TRUST	2915 Jorie Boulevard, Oak Brook, IL 60523	2
OMRON MANAGEMENT CENTER OF AMERICA GROUP HEALTH PLAN	2895 Greenspoint Pkwy #100, Hoffman Estates, IL 60169	3
THE COVENANT CHURCH GROUP HEALTH PLAN	8303 W Higgins Road, Chicago, IL 60631	2

DELTA DENTAL

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Notice of Data Breach

Delta Dental of Illinois is writing to inform you of a security incident that may have involved certain personal information of yours and/or that of your covered dependents. We are providing this notice as a precaution to inform potentially affected individuals about the incident. To assist you with any concerns you may have about this incident, we are offering you one year of identity theft protection and monitoring through Experian's® IdentityWorks® and highlighting some additional steps you can take to help protect yourself. We deeply regret this incident occurred and are committed to safeguarding our members' personal information.

What Happened

We recently learned that an outside individual sent phishing emails to certain Delta Dental of Illinois employees soliciting their login information to our email system. The outside individual obtained and used the email credentials of one employee to gain unauthorized access to that employee's email account. Though we do not have evidence that the outside individual actually viewed or used the contents of the email account, results of our third-party forensic investigation showed that this individual did have access to the email account between December 21 and December 28, 2018. Following the investigation, we finalized the data review and discovered who the impacted members were on March 1, 2019.

What Information Was Involved

The information stored in the affected employee's email account varied by individual, but may have included first and last names, addresses, dates of birth, dental or vision insurance information and/or Social Security numbers. Based on our investigation, it appears you are one of the individuals whose information was stored in the account, and therefore your information could be affected by this incident. Our investigation has not found any evidence that this incident involved any unauthorized access to or use of any of Delta Dental of Illinois' internal computer systems or network, or that any other information

was affected. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

Delta Dental of Illinois takes our obligation to protect the privacy and security of our members' personal information seriously. After this incident was discovered, we promptly took steps to address this situation, including initiating an internal investigation and retaining an independent forensic investigation firm to assist us in our investigation of and response to this incident. Additionally, we have reset employee account passwords and implemented additional email security tools to help prevent this type of incident from reoccurring in the future. We have also consulted with law enforcement.

To help protect your identity, we are offering one year of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions in the "Information about Identity Theft Protection" reference guide included with this letter.

What You Can Do

Although we are not aware of any misuse of your information as a result of this incident, we want to make you aware of steps that you can take as a precaution:

- **Activate the Complimentary Identity Protection Services.** As outlined above, we are offering one year of identity theft protection and credit monitoring services through Experian's® IdentityWorks® at no charge to you. For more information about these services and instructions on completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter. **Note that you must complete the enrollment process by June 30, 2019.**

- **Check Credit Reports and Financial Accounts.** You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.

- **Review Explanation of Benefits Documents.** You can also review explanation of benefits statements that you receive from Delta Dental of Illinois or review for persons whose dental or vision bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits that were not received, please immediately contact us.

- **Consult the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included with this letter, which describes additional

steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact our dedicated call center at 855-540-5615 between the hours of 9 am and 9 pm Eastern Time, Monday through Friday. Additionally, we have provided some additional information and resources about protecting information on our website at www.deltadentalil.com/2019-data-incident/. Again, we take our obligation to protect our members' personal information seriously and regret any concern that this incident may cause.

Sincerely,

John Maples

John Maples
President and CEO

**DeltaVision is provided by ProTec Insurance Company, a wholly-owned subsidiary of Delta Dental of Illinois, in association with EyeMed Vision Care networks.*

Information about Identity Theft Protection

To help protect your identity, we are offering a complimentary membership in Experian's® IdentityWorks®. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. Included with this service are fraud resolution services that provide an Experian Fraud Resolution agent to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). While this Fraud Resolution assistance is immediately available to you without any further action on your part, you can also activate the fraud detection tools available through enrolling in IdentityWorks® at no cost to you. To enroll in these services, visit: **www.experianidworks.com/3bcredit** by **June 30, 2019**, and use the following activation code: **[ACTIVATION CODE]**. You may also enroll over the phone by calling **877-890-9332** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **DB11132.**

Once you enroll in IdentityWorks, you will have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[1]:** Provides coverage for certain costs and unauthorized electronic fund transfers

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

---

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Information About Medical Identity Theft: Patients who pay for medical services can regularly review the explanation of benefits (EOB) statements that they receive from their health insurers or health plans. If they identify services listed on the EOB that were not received, they should immediately contact the health plan. For more information about protecting yourself from the Department of Health and Human Services, please visit https://oig.hhs.gov/fraud/medical-id-theft.

Security Freezes and Fraud Alerts: You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity;

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and

(4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)

General Contact:

P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374
Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
General Contact:

P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact:

P.O. Box 105281
Atlanta, GA 30348
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872