



December 29, 2023

VIA EMAIL [IDTHEFT@OAG.STATE.MD.US]

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Notice Pursuant to MD Commercial Code § 14–3501(e)

Dear Attorney General Brown:

Pursuant to **Maryland Commercial Code section 14–3501(e)**, we write on behalf of EDI Health Group dba DentalXChange Holdings, LP (“DentalXChange” or “Company”) to notify you of a data security matter, which we believe may have affected approximately two (2) Maryland residents.

On or around August 11, 2023, DentalXChange became aware of unauthorized activity in a user account for an associated dental practice. In response, DentalXChange initiated a comprehensive investigation into the matter with the assistance of third-party specialists. After an extensive review of the activity, DentalXChange identified that certain dental practice accounts were accessed by an unauthorized party. DentalXChange’s review did not reveal evidence that individuals’ data was accessed by this party, but that potential cannot be ruled out. DentalXChange then conducted a comprehensive evaluation of the potentially impacted accounts to determine what patient information was contained therein and, subsequently, to identify the current mailing address for potentially impacted individuals. This process was completed on or around December 26, 2023. Based on DentalXChange’s review, they determined that the potentially impacted accounts may have included personal information of Maryland residents.

The types of information that may have been impacted will depend on the information provided to DentalXChange from current and former dental providers about the individual, but may include: name, address, date of birth, and insurance information including subscriber ID and list of dental procedures. Notification of this matter will be mailed to the impacted residents on or around January 2, 2023. A copy of this notification is attached as **Exhibit A**.

DentalXChange takes the protection of information seriously. DentalXChange is offering two years of identity protection services, at no cost, to affected individuals through IDX. DentalXChange has taken steps in an effort to prevent a similar incident during this process.

Below is the contact information for Bill Dachelet, Information Security Officer:

(800) 576-6412, Ext. 149
bdachelet@dentalxchange.com



Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,

L. Judson Welle, Partner

DentalXChange
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB08301 1-1



name
address
Edmond, OK 73013-5349
|||||

January 2, 2023

RE: NOTICE OF DATA BREACH

Dear name,

We are contacting you regarding a security incident at EDI Health Group dba DentalXChange (“DentalXChange”) that may have impacted some of your information. The DentalXChange platform is used by dental practices to file insurance claims for dental procedures. Your current or former dental provider used DentalXChange for such services. We are providing you with information about this matter and steps you may take to help protect your information. Please be aware that, at this time, there is no evidence that your information has been accessed or misused as a result of this incident.

What Happened

On or around August 11, 2023, DentalXChange became aware of unauthorized activity in a user account for an associated dental practice. In response, DentalXChange initiated a comprehensive investigation into the matter with the assistance of third-party specialists. After an extensive review of the activity, DentalXChange identified that certain dental practice accounts were accessed by an unauthorized party. Our review did not reveal evidence that your data was accessed by this party, but that potential cannot be ruled out. We then conducted a comprehensive evaluation of the potentially impacted accounts to determine what patient information was contained therein and, subsequently, to identify the current mailing address for potentially impacted individuals. This process was completed on or around December 26, 2023.

What Information Was Involved

The types of information that may have been impacted depend on the information provided to DentalXChange by your current or former dental provider, but may include all data elements found on a Dental Claim Form including your name, address, date of birth, and insurance information including subscriber ID and list of dental procedures.

What We Are Doing

DentalXChange takes the security of your information very seriously. Upon learning of the security incident, we immediately launched an internal investigation and took steps to prevent further unauthorized access. DentalXChange has also hired a respected forensics investigation firm to help identify and prevent any further unauthorized access and consulted with federal law enforcement in support of our investigation and response to this matter. In addition, to help you protect your information, we are providing you with **free identity protection services for two years**, as described in the document attached to this letter.

What You Can Do

There are steps you can take to help protect your information, including enrolling in the identity protection service we are offering to you for free. We are providing you with 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 24 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/dxc> and follow the instructions provided. When prompted please provide the following unique code to receive services: **RWV3CDXW43**

In order for you 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.

Again, at this time, there is no evidence that your information has been accessed as a result of this incident, but we encourage you to follow best practices and remain vigilant for suspicious activity and to regularly review your financial statements and credit reports. In order to take advantage of free identity protection service for two years, please review the information attached to this letter. TransUnion representatives can answer questions or concerns you may have regarding these services and the protection of your information.

For More Information

In addition to the information provided in this letter, we have also enclosed an attachment with additional information and resources. Please note, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please retain this letter for your enrollment.

If you have any additional questions, you can call 1-833-760-0556 from 8:00 am to 8:00 pm ET, Monday through Friday, excluding holidays.

Sincerely,



Paul Kaiser
Chief Executive Officer
DentalXChange

ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission (“FTC”), the credit reporting agencies, or your state’s regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax

PO Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian

PO Box 4500
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

PO Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau’s website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and 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 FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a “credit freeze”). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which are actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the 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