

Stacy A. Cole
Partner
Direct: 513.629.2838
scole@graydon.law


GRAYDON
2400 Chamber Center Drive
Suite 300
Ft. Mitchell, KY 41017
Main 859 282 8800
Fax 859 525 0214

May 26, 2022

BY EMAIL TO idtheft@oag.state.md.us

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Data Incident Report

To the Attorney General:

The purpose of this correspondence is to report a data incident that occurred at the City of Cincinnati (Ohio) (the “City”). For correspondence purposes, this incident is reported by:

Stacy A. Cole
Graydon Head & Ritchey LLP
2400 Chamber Center Drive, Suite 300
Ft. Mitchell, KY 41011
Phone: 513.629.2838
Email: scole@graydon.law

The organization reporting the incident is:

City of Cincinnati
805 Central Avenue, Suite 100
Cincinnati, Ohio 45202
www.cincinnati-oh.gov

One Maryland resident may have been impacted by the incident. The City is mailing written notification to this individual on May 27, 2022.

On April 19, 2022, the City of Cincinnati discovered that a Request for Proposal (“RFP”) for vision and dental services that inadvertently included participant census data was posted on the City’s procurement websites. The RFP was posted on April 8, 2022 at 4pm, and was removed upon discovery on April 19, 2022. The census files contained in the posted RFP included personal and protected health information (“PHI”) of prior or current participants in the City’s dental and/or vision programs. This data included name, home address, demographics information, vision and/or dental insurance information such as ID numbers and membership terms, and in some cases, Social Security number (SSN), dental claims information, and date of birth. Credit card information, banking information, or medical information such as test results or treatment records, was not



compromised. Dental claims information was not included in the RFP for the one of the five impacted Virginia residents.

The City, in conjunction with its healthcare consultant, immediately launched an investigation into the circumstances surrounding the posted RFP and determined that the census files were included by mistake. This incident was not the result of a cybersecurity breach or malware attack. The City's investigation has also involved obtaining the number of downloads of the RFP and attempting to trace IP addresses. The City has requested deletion, among other certifications, from any parties that have been identified as potentially downloading the data.

The City takes the protection of personal information seriously and is taking steps to prevent a similar occurrence. The City, in conjunction with its healthcare consultant, immediately launched an investigation into the circumstances surrounding the posted RFP and determined that the census files were included by mistake. The City's investigation has also involved obtaining the number of downloads of the RFP and attempting to trace IP addresses. The City has requested deletion, among other certifications, from any parties that have been identified as potentially downloading the data. In addition, the City is reviewing its policies and processes for RFPs and sensitive information handling, and is implementing additional training. The City is also working with its healthcare consultant to apply additional protocols and training regarding information sharing practices. The City's investigation has found no indication or evidence that any personal information or PHI has actually been misused or otherwise compromised. Nonetheless, the City is handling this matter with an abundance of caution.

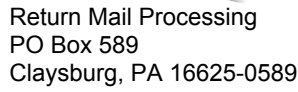
The City originally sent notifications with two years of complimentary credit monitoring and identity restoration services from Experian to all then-identified impacted individuals on May 13, 2022. No Maryland residents were included in that original mailing. Since then, the City has identified additional individuals impacted by the incident. These include a number of additional dependents, who are being offered the two-year credit monitoring and identity restoration services as described herein.

The remaining individuals are dental services providers included on a claims file, some of whom used their SSN as their business Tax ID number. For those who were identified as using their SSN, or who may have been using their SSN, they were offered one year of credit monitoring. For those who were confirmed as not using their SSN as their Tax ID number, they are being notified, but not offered credit monitoring. The one Maryland resident impacted is a dental provider who was not using a SSN as a business Tax ID number. If there are further questions or requests for information, please let us know.

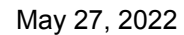
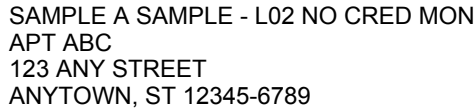
Very truly yours,

GRAYDON HEAD & RITCHEY LLP

Stacy A. Cole



H9287-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345



Dear Sample A. Sample:

The City of Cincinnati (the "City") recently discovered an incident that may affect the security of your personal information. Because the City is committed to transparency and takes the protection and proper use of your information very seriously, the City is providing you with information about the incident, steps the City is taking in response, and steps you may take to guard against identity theft and fraud.

What Happened? On April 19, 2022, the City discovered that a Request for Proposal (“RFP”) for vision and dental services inadvertently included participant census data that was posted on the City’s procurement websites. The RFP was posted on April 8 at 4pm, and was removed upon discovery on April 19. Please be assured that the City has taken every step necessary to address the incident.

What Information Was Involved? The census files contained in the RFP included information relating to dental claims and providers, including name, address, claim amounts, and tax ID number. Banking or other financial information, and your Social Security number were NOT released. The City's investigation has found no indication or evidence that any personal information has actually been misused or otherwise compromised. Nonetheless, the City is handling this matter with an abundance of caution.

What Is The City Doing? The City takes the protection of your personal information seriously and is taking steps to prevent a similar occurrence. The City, in conjunction with its healthcare consultant, immediately launched an investigation into the circumstances surrounding the posted RFP and determined that the census files were included by mistake. This incident was not the result of a cybersecurity breach or malware attack. The City's investigation has also involved obtaining the number of downloads of the RFP and attempting to trace IP addresses. The City has requested deletion, among other certifications, from any parties that have been identified as potentially downloading the data.

What You Can Do. The City recommends that you remain vigilant for incidents of fraud and identity theft, including reviewing account statements and monitoring free credit reports. You can obtain information from the Federal Trade Commission and consumer reporting agencies about fraud alerts and security freezes, as described in the enclosed *Information about Identity Theft Protection*. Please review this enclosure for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary identity protection services being offered.

For More Information. The City sincerely regrets any inconvenience or concern caused by this incident. If you have further questions or concerns, please call 800-422-8339 toll-free Monday through Friday from 8:00 a.m. to 5:00 p.m. EST.

Sincerely,

Deborah Allison
Risk Manager

H9287-L02

Information About Identity Theft Protection

Monitor Your Accounts

The City recommends that you 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 below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and 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. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
[www.experian.com/
fraud/center.html](http://www.experian.com/fraud/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
[www.transunion.com/fraud-
victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Monitor Your Personal Health Information

If applicable to your situation, the City recommends that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

If you are a California resident, the City suggests that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

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

You should also be aware of scam email campaigns that may target current and former City employees. These scams, designed to capture personal information (known as “phishing”), are designed to appear as if they are from the City and the emails may include a “click here” link for credit monitoring. These emails are NOT from the City. DO NOT reply to the email or reach out to the senders in any way; DO NOT supply any information on the website that may open, if you have clicked on an email link; and DO NOT open any attachments in the email.

The City is not calling individuals regarding this incident and is not asking for credit card information or Social Security numbers over the phone. For more guidance on recognizing scam email, please visit the FTC Website: <http://www.consumer.ftc.gov/articles/0003-phishing>.

District of Columbia residents may also wish to review information provided by the Attorney General for the District of Columbia on how to avoid or recover from identity theft at <https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft>, or at the Office of the Attorney General, 400 6th Street NW, Washington, DC 20001, oag@dc.gov, (202) 727-3400.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid or recover from identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or at the Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, idtheft@oag.state.md.us, 410-576-6491.

New York residents may also wish to review information provided by the New York Attorney General on how to avoid or recover from identity theft at <https://ag.ny.gov/internet/privacy-and-identity-theft>, or at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, ifraud@ag.ny.gov, 212-416-8433.

North Carolina residents may obtain free information about steps you can take to prevent identity theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/> or at North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

0000002

