



ROPES & GRAY LLP
2099 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20006-6807
WWW.ROPESGRAY.COM

October 4, 2023

Fran Faircloth
T +1 202 508 4788
fran.faircloth@ropesgray.com

BY E-MAIL

Attorney General Anthony Brown
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Data Incident

Dear Attorney General Brown:

We write on behalf of our client, Heartland Dental, to inform you of a recent security incident that may have affected the personal information of 3 Maryland residents.

On or about March 16, 2023, an unauthorized individual(s) (the "intruder") gained access to the Heartland Dental employee portal and altered the financial account information of several Heartland Dental employees. Upon learning of the intrusion, Heartland Dental promptly initiated an internal investigation, reset the login credentials of the affected employees, and removed the intruder. Heartland Dental concluded its investigation on July 27, 2023.

During the course of the investigation, Heartland Dental provided a preliminary notice via email to individuals who were expected to be affected. This included the 3 Maryland residents. Now that the investigation is complete, Heartland Dental is providing those employees with the attached notice letter, which includes information on credit monitoring services and a telephone number consumers may call for further information and assistance. If you have any questions, please reach out to us at +1 (202)-508-4788.

Sincerely,

A handwritten signature in blue ink, appearing to read "Fran Faircloth".

Fran Faircloth

October 4, 2023

[Recipient Name]
[Recipient Address]
[Recipient City, State, Zip]

RE: Notice of Security Incident

Dear [Name]:

We are writing to follow up on a previous email you received on April 21, 2023 regarding an incident involving your personal information. In the interest of time, we provided you with the preliminary email notification while we were still investigating the incident. In this notice, you will find information about the incident, the response, and steps you may take to further protect your personal information.

What Happened?

On or about March 16, 2023, an unauthorized individual(s) (the “intruder”) gained access to the Heartland Dental employee portal and altered the financial account information of several Heartland Dental employees. Upon learning of the intrusion, Heartland Dental promptly initiated an internal investigation, reset the login credentials of the affected employees, and removed the intruder.

Heartland Dental is providing this notice to you as our records indicate that your personal information may have been accessible to the unauthorized individual(s).

What Information Was Involved?

While Heartland Dental has confirmed that the intruder would not have had access to any individual’s protected health information, it appears that the intruder may have accessed your personal information in the employee portal. This information varied depending on the individual but may have included your first and/or last name; date of birth; social security number; or financial account number(s).

What Are We Doing?

Heartland Dental takes this incident and the security of your information very seriously. Upon learning of the incident, Heartland Dental launched an internal investigation to assess the intrusion. In addition, Heartland Dental promptly changed the log-in credentials of all affected employees and performed a forced log out of the affected employee accounts to prevent any unauthorized individual(s) from further accessing the employee portal. Heartland Dental has also taken steps to enhance information security, including requiring that all Heartland Dental workforce members update their log-in credentials.

The privacy and security of your information is a priority of Heartland Dental. We will continue to monitor our information security systems and make improvements and enhancements where appropriate.

As an added precaution, Heartland Dental is also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services. If you wish to receive these services, activation instructions are below. We are making free credit monitoring available to you out of an abundance of caution in case you find it useful, but we do not intend to suggest that your personal data are at risk of misuse.

What Can You Do?

We encourage you to regularly review your financial accounts and report any suspicious or unrecognized activity immediately. As recommended by federal regulatory agencies, you should remember to be vigilant for the next 12 to 24 months and report any suspected incidents of fraud to the relevant financial institution.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident. Experian Identity Restoration is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we are also offering complimentary access to Experian IdentityWorksSM for one year. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 30, 2023** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: [Activation Code]**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by November 30, 2023. Be prepared to provide engagement number **B103692** as proof of eligibility for the identity restoration services by Experian.

Other Important Information.

We apologize for the inconvenience that this incident may cause. We take all data security matters seriously and are taking steps to minimize the chances of a similar occurrence happening again.

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call (217) 540-5167.

Sincerely,

Craig Kabbes, EVP & Chief Information Officer

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Important Identity Theft Information

Additional Steps You Can Take to Protect Your Identity

Review Your Accounts and Credit Reports

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®
1-888-378-4329
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion®
1-800-916-8800
www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a “fraud alert” be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax®
1-877-478-7625
www.equifax.com/personal/credit-report-services/credit-fraud-alerts

Experian
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion®
1-800-680-7289
www.transunion.com/fraud-alerts

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. It is free to place, lift or remove a security freeze.

You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

Equifax®
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-378-4329
www.equifax.com/personal/credit-report-services/credit-freeze

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

TransUnion®
P.O. Box 160
Woodlyn, PA 19094
1-800-916-8800
www.transunion.com/credit-freeze

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies and include (1) proper identification; (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Suggestions If You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idtheft04.pdf>.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft at: <http://www.ftc.gov/idtheft>; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State Specific Information

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

New York residents can learn more about security breach response and identity theft prevention and protection from the New York State Department of State Division of Consumer Protection, by visiting their web site at <https://dos.ny.gov/protecting-yourself-identity-theft>, calling 1.800.697.1220 or by contacting federal agencies using the contact information listed above.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.