BakerHostetler

Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Sara M. Goldstein
direct dial: 215.564.1572
sgoldstein@bakerlaw.com

October 19, 2022

VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)

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

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, Oklahoma Lions Sight Conservation Foundation, Inc. dba Oklahoma Lions Eye Bank ("Oklahoma Lions Eye Bank"), to notify your office of a cybersecurity incident.

Oklahoma Lions Eye Bank recently concluded its investigation of a data security incident that involved unauthorized access to several employees' email accounts. Oklahoma Lions Eye Bank became aware of the incident when they learned that a payment made on an invoice was not received by the recipient. After identifying the incident, Oklahoma Lions Eye Bank immediately secured the accounts in its email system, reset email account passwords, and launched an investigation. Through its investigation, it was determined that an unauthorized party had gained access to the employee email accounts between April 18, 2022 and May 6, 2022, and during this time, sent emails from one of the accounts in an attempt to obtain funds from Oklahoma Lions Eye Bank through a fraudulent wire transfer. Although the likely purpose of the unauthorized access to the employee email accounts was to obtain funds from Oklahoma Lions Eye Bank through a fraudulent wire transfer, not to access personal information, Oklahoma Lions Eye Bank cannot rule out the possibility that emails and attachments in the accounts may have been accessed as a result of this incident. On September 20, 2022, Oklahoma Lions Eye Bank determined that the files contained information related to three Maryland residents, including those individuals' names and Social Security numbers.

On October 19, 2022, Oklahoma Lions Eye Bank mailed notification letters via United States Postal Service First-Class mail to individuals whose information may have been involved in accordance with Md. Code Ann., Com. Law § 14-3504. A sample copy of the notification letter is enclosed.[1] Oklahoma Lions Eye Bank is offering notified residents complimentary memberships to credit monitoring and identity protection services through Experian. Oklahoma Lions Eye Bank also provided a direct phone number to answer question that individuals may have.

To help prevent a similar incident from occurring in the future, Oklahoma Lions Eye Bank is continuing to enhance its existing email security practices and protocols.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Sara Goldstein

Sara M. Goldstein
Partner

Enclosure

[1] This report does not waive Oklahoma Lions Eye Bank's objection that Maryland lacks personal jurisdiction over it related to any claims that may arise from this incident.

[redacted]

October 19, 2022

[redacted]

Oklahoma Lions Sight Conservation Foundation, Inc. dba Oklahoma Lions Eye Bank ("Oklahoma Lions Eye Bank") is committed to protecting the confidentiality and security of the information we maintain. We are writing to inform you about an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On August 8, 2022, Oklahoma Lions Eye Bank concluded our investigation of a data security incident that involved unauthorized access to several employees' email accounts. We became aware of the incident when we learned that a payment we made on an invoice was not received by the recipient. After identifying the incident, we immediately secured the accounts in our email system, reset email account passwords, and launched an investigation. Through our investigation, we determined that an unauthorized party had gained access to the employee email accounts between April 18, 2022 and May 6, 2022, and during this time, sent emails from one of the accounts in an attempt to obtain funds from Oklahoma Lions Eye Bank through a fraudulent wire transfer. Although the likely purpose of the unauthorized access to the employee email accounts was to obtain funds from Oklahoma Lions Eye Bank through a fraudulent wire transfer, not to access personal information, we cannot rule out the possibility that emails and attachments in the accounts may have been accessed as a result of this incident. Therefore, out of an abundance of caution, we conducted a review of emails and attachments in the Oklahoma Lions Eye Bank employee email accounts.

Based on this review, we determined that the accessible emails and attachments contained information about you and may have been accessed as a result of this incident. This information includes your name in combination with your Social Security number and medical treatment information.

We recommend that you remain vigilant to the possibility of fraud by reviewing your financial account statements for any suspicious activity. We recommend that you immediately report any suspicious activity to your financial institution. We also recommend that you regularly review the statements you receive from your health care providers. If you see services that were not received, you should contact the provider immediately. As a precaution, we are offering you a complimentary one-year membership to Experian® IdentityWorks℠ Credit 3B. **For more information on Experian IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership and steps you can take to protect your information, please see the pages that follow this letter.**

We sincerely regret any inconvenience or concern this may cause you. Oklahoma Lions Eye Bank takes this incident very seriously and, as part of our ongoing efforts to help prevent something like this from happening in the future, we are continuing to enhance our existing email security practices and protocols.

If you have any questions, please call 405-557-1393, ext 100, Monday through Friday, 8:30 a.m. and 3:30 p.m., Central Time.

Sincerely,

Lori A. Miller

Lori A. Miller, CEBT
Executive Director

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. 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.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **January 31, 2023** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: https://www.experianidworks.com/3bcredit
3. PROVIDE the Activation Code: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.890.9332. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH
EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian immediately without needing to enroll in the product regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

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

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

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877.890.9332 to register with the activation code above.

What you can do to protect your information: 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. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877.890.9332.

* 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. Please refer to the actual policies for terms, conditions, and exclusions of coverage.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Oklahoma Lions Eye Bank's mailing address is 3840 N. Lincoln Blvd., Oklahoma City, Oklahoma 73105, and its phone number is 405-557-1393.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.