



Ryan M. Cook
24 Greenway Plaza, Suite 1400
Houston, Texas 77046
Ryan.Cook@lewisbrisbois.com
Direct: 346.241.4107
*Not yet licensed in Texas

March 27, 2023

Via electronic-mail: *ldtheft@oag.state.md.us*

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

Re: Our Client: Oklahoma City University
Matter: July 2022 Data Security Incident

Dear Attorney General Brown:

We represent Oklahoma City University ("OCU"), located in Oklahoma City, Oklahoma, with respect to a data security incident described in more detail below. OCU takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that OCU has taken in response to this incident. We have also enclosed hereto a sample of the notification made to the potentially impact individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On July 23, 2022, OCU detected and stopped a network security incident. OCU immediately shut off all access to the network and engaged a specialized third-party forensic incident response firm to assist with securing the environment. OCU's network has been secured and remediated. OCU initiated a comprehensive investigation into what sensitive data could have been compromised.

Although OCU found no evidence that individuals' personal information has been specifically misused, it is possible that individuals' full name, mailing address, social security number, passport number, and driver license/state ID number could have been exposed to the cybercriminal.

As of this writing, OCU has not received any reports of related identity theft since the date of the incident.

2. Maryland Residents Notified

A total of eighty three (83) Maryland residents were potentially affected by this security incident. Notification letters were mailed to these individuals on March 20, 2023 by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon detecting this incident, OCU moved quickly to initiate a response, which included engaging third-party cybersecurity and IT specialists to secure OCU's network environment and conduct a comprehensive investigation into the incident. OCU has reported this incident to law enforcement. OCU has reviewed and altered its policies and procedures relating to the security of its systems and servers, as well as its information life cycle management.

Although OCU is not aware of any evidence of misuse of personal information, OCU extended to potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include 12 months of credit monitoring, along with a fully managed ID theft recovery service, should the need arise.

4. Contact Information

OCU remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact Ryan M. Cook, Esq. at: Ryan.Cook@LewisBrisbois.com or 346.241.4107.

Sincerely,



Ryan M. Cook for
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: *Sample notification letter*

RMC



Return to IDX:
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-753-4675
Or Visit:
<https://response.idx.us/ocu>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

March 20, 2023

Via First-Class Mail

Notice of Data Security Incident

Dear <<FIRST NAME>> <<LAST NAME>>,

We are writing to inform you of a data security incident that may have resulted in unauthorized access to your personal information. We take the privacy of your personal information seriously, and want to provide you with information and resources you can use to protect your identity. This letter contains information about the incident and information about how to protect your personal information going forward.

What Happened and What Information was Involved:

On July 23, 2022, Oklahoma City University ("OCU") detected and stopped a network security incident. An unauthorized third-party infiltrated our network and encrypted some of our data. We immediately shut off access to the impacted systems and engaged specialized third-party forensic and technical resources to respond to the incident. OCU has since secured its network and the data that we maintain.

Through our ongoing investigation, the university recently has learned that the unauthorized party obtained some personal identifiable information of current and prior students and others with information held on the university's systems. The following categories of your information may have been exposed to the unauthorized party during the compromise: Name, Address, Social Security Number, Driver's License/State ID Number, and Passport Number. Notably, the types of information affected varied by individual, and not every individual had every element exposed. There currently is no indication that this information has been misused.

As of this writing, OCU has not received any reports of related identity theft since the date of the incident.

What We Are Doing:

OCU is committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon detecting this incident, we moved quickly to initiate our incident response program, which included fully securing our network and the data that we maintain. We conducted an investigation with the assistance of third-party forensic specialists and have reported this matter to law enforcement. We are reviewing our tools, policies, and procedures relating to the security of our systems and servers.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you

resolve issues if your identity is compromised.

What You Can Do:

We encourage you to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-753-4675 or going to <https://response.idx.us/ocu> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is June 20, 2023.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

You will find detailed steps for protecting your information on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-753-4675 or go to <https://response.idx.us/ocu> for assistance or for any additional questions you may have.

Sincerely,



Kenneth R. Evans, President
Oklahoma City University

(Enclosure)

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-alerts

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at:

600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov