

September 6, 2023

Via Electronic Mail Only

Maryland Attorney General's Office

Idtheft@oag.state.md.us

Re: Oklahoma Baptist University - Cyber

To Whom It May Concern:

The purpose of this letter is to comply with MARYLAND CODE, COMMERCIAL LAW, § 14-3504, and to inform you of a cyber incident at Oklahoma Baptist University ("OBU") located in Oklahoma.

WHAT HAPPENED

As part of a nationwide attack against universities, on April 28, 2023, and June 1, 2023, an unauthorized third party initiated ransomware attacks on university networks across the country including OBU's computer network. In response, OBU immediately shut down its network and launched an investigation. On June 15, 2023, OBU discovered that the unauthorized third party obtained access and may have exfiltrated some data from certain servers containing PII. On August 1, 2023, OBU was able to identify all individuals whose PII may have been accessed or exfiltrated.

WHAT INFORMATION WAS INVOLVED

The information accessed by the unauthorized user included information for twenty-six (26) Maryland residents and may have included their name and social security number.

WHAT OBU IS DOING TO PROTECT ITS MARYLAND RESIDENTS

On August 31, 2023, OBU sent notification letters to the affected Maryland residents offering identity theft protection services through IDX, the data breach and recovery services expert, including 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity recovery services. A copy of the template notification is attached. The credit monitoring service will provide affected residents with the necessary tools to resolve issues if any of them have their identity compromised.

WHAT OBU IS DOING TO IMPROVE CYBER SECURITY

OBU is enhancing its administrative and technical security protocols including network upgrades, multi-factor authentication, and data encryption.

OBU is committed to maintaining the privacy and security of students and/or prospective students personal identifiable information and will cooperate fully. Please contact me directly if you need additional information. Thank you.

Sincerely,

RIGHI FITCH LAW GROUP



Elizabeth S. Fitch
Melissa Lin
For the Firm

ESF/ML:cm

Enclosure: notification letter template



P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/OBU>

August 31, 2023

Notice of Data Breach

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

Oklahoma Baptist University (“OBU”) is not only committed to equipping students to pursue academic excellence, integrate faith with all areas of knowledge, engage a diverse world, and live worthy of the high calling of God in Christ, but also committed to transparency, integrity, and maintaining the privacy and security of your personally identifiable information (PII). Because of that commitment, we need to inform you of a recent cybersecurity incident. Unfortunately, as part of a nationwide attack against universities, on April 28, 2023, and June 1, 2023, an unauthorized third party initiated ransomware attacks on university networks across the country and OBU’s computer network was attacked as well. In response, we immediately shut down our network and launched an investigation. We engaged a group of outside IT solution experts to eradicate the ransomware and to rebuild, restore, and upgrade the security of our network.

What Happened

Since the discovery of the ransomware attack, our internal IT Support, outside solutions experts, and other OBU employees have been working tirelessly to contain the ransomware, restore the network, and improve security controls. Our IT experts have confirmed that the ransomware has been contained and that the network has been fully rebuilt and restored. On June 15, 2023, we discovered that the unauthorized third party obtained access and may have exfiltrated some data from certain servers containing PII. On August 1, 2023, we were able to identify all individuals whose PII may have been accessed or exfiltrated. We regret to inform you that some of your personally identifiable information may have been accessed or exfiltrated. While we have no reason to believe that your information has been misused, we believe it is prudent to notify you and provide additional protection. We have decided to take the precautionary step of offering you CyberScan dark web monitoring and/or credit monitoring for a year. We deeply regret this incident and any inconvenience to you and recommend you contact the number below for more information. This ransomware attack was a highly organized effort against multiple universities across the country. Many of these institutions were completely immobilized or severely debilitated. OBU’s team of specialists was able to restore OBU systems and services quickly and we remain committed to pursuing the mission of OBU on campus, in our community, and throughout the world.

What Information Was Involved

The information accessed by the unauthorized user may have included your name and social security number.

What We Are Doing

We are taking additional steps to protect your PII from access and other unauthorized activity in the future. We are

enhancing our administrative and technical security protocols including network upgrades, multi-factor authentication, and data encryption.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity 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 contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-996-4098, or going to <https://response.idx.us/OBU>, or scanning the QR image 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 November 30, 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.

For More Information

You will find detailed instructions for enrollment 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 1-888-996-4098 or go to <https://response.idx.us/OBU> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read 'Joshua Shoffner', with a long horizontal flourish extending to the right.

Joshua Shoffner
Vice President of Technology and Digital Innovation
Oklahoma Baptist University

(Enclosure)



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/OBU> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-996-4098 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.