[redacted]

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

Re: Notice of Security Incident

To whom it may concern:

On behalf of Oklahoma Baptist University ("OBU"), we are notifying your office of a data security incident potentially involving the information of two (2) Maryland residents.

On Friday, January 21, 2022, OBU learned that an internal file that included personal information about student enrollees had been improperly stored on a file server by OBU staff causing the file to be generally accessible to OBU students and employees with access to OBU's intranet. Information in the file included student ID numbers, names, addresses, birthdate, gender, phone numbers, social security numbers, educational history (such as historical GPA, admission history and the like) of the students identified in the record. Our understanding is that your office wishes for notice of such incidents prior to individual/consumer notification letters being sent. Such notification letters, in the form attached, are expected to be sent on or by February 14, 2022.

Immediately upon learning of the situation, OBU staff removed the file-at-issue from general OBU accessibility and investigated the matter to ensure, as best as possible, that the personal information involved was not exposed to fraud or other unlawful activity. That investigation included contacting internal staff members involved, reviewing file logs to determine access, and interviewing those believed to have had such access. Based on its investigation, OBU believes eight individuals (all OBU students or employees) accessed the file while it was improperly stored and the interviews conducted by OBU yielded no evidence of improper use or storage of the information in the file. As a result, OBU believes the incident has been contained and the file and its information prevented from further unauthorized access.

If you have any questions, or need further information, please let me know.

Sincerely,
-Zach Oubre

Zachary A.P. Oubre
Attorney
(405) 270-6023 direct
(405) 228-7622 assistant
(405) 270-7223 fax
zach.oubre@mcafeetaft.com
VCard | BIO | www.mcafeetaft.com

For information and assistance navigating the COVID-19 crisis, please visit our COVID-19 Resource Center at: https://www.mcafeetaft.com/covid-19-resource-center/

OKBU.EDU

500 West University | Shawnee, OK 74804

February 14, 2022

Via First Class Mail
[Student's Name]
[Address Line 1]
[Address Line 2]
[City, State] [Zip]

INFORMATION SECURITY NOTIFICATION

We are writing to let you know about a data security incident that involved personal information of yours maintained by Oklahoma Baptist University ("OBU" or "we") as discussed below. Importantly, we are currently unaware of any actual misuse of your information and, based upon our investigation, have no reason to believe there has been or will be unauthorized use of your personal information as a result of this incident. Nevertheless, we are reaching out to you so that you may take all measures you deem necessary to protect against possible identity theft, fraud and other unlawful or unauthorized conduct.

What Happened and What Information Was Involved.

On Friday, January 21, 2022, we learned that an internal OBU file that included personal information about student enrollees had been improperly stored on a file server by OBU staff causing the file to be generally accessible to OBU students and employees with access to OBU's intranet. Information in the file included student ID numbers, names, addresses, birthdate, gender, phone numbers, social security numbers, educational history (such as historical GPA, admission history and the like) of the students identified in the record. Your information was included in this file which is the reason for this notice. The file-at-issue was not accessible to the general public lacking OBU log-in access to our intranet.

What We Are Doing.

Immediately upon learning of the situation, OBU staff removed the file-at-issue from general OBU accessibility and investigated the matter to ensure, as best as possible, that the personal information involved was not exposed to fraud or other unlawful activity. That investigation included contacting internal staff members involved, reviewing file logs to determine access, and interviewing those believed to have had such access. Based on our investigation, we believe eight individuals (all OBU students or employees) accessed the file while it was improperly stored and the interviews conducted by OBU yielded no evidence of improper use or storage of the information in the file. As a result of OBU's efforts, we believe the incident has been contained and the file and its information prevented from further unauthorized access; however, we encourage you to be diligent in monitoring for any suspicious activity concerning your information.

Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for one (1) year provided by Kroll. Please see the handout enclosed with this letter for enrollment instructions.

What You Can Do.

Also included at the end of this letter is a handout entitled "Steps You Can Take to Protect Your Information". You may use the contact information set forth therein to contact credit reporting and other agencies about fraud alerts, security freezes and other ways to protect against identity theft and other misuse of your personal information.

For More Information.

If you have further concern about this incident, or need any further assistance, please contact us [**(XXX) XXX-XXX**, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. We will endeavor to respond to your inquiries in a timely fashion. We sincerely regret any inconvenience or concern caused by this incident.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

Review your financial account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint with the FTC, go to *IdentityTheft.gov* or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

You should obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting *http://www.annualcreditreport.com*, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at *https://www.annualcreditreport.com/requestReport/requestForm.action*. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

- **Equifax**, (866) 349-5191, *www.equifax.com*, P.O. Box 740241, Atlanta, GA 30374
- **Experian**, (888) 397-3742, *www.experian.com*, P.O. Box 2002, Allen, TX 75013
- **TransUnion**, (800) 888-4213, *www.transunion.com*, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Take Advantage of Additional Free Resources on Identity Theft

Review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit *IdentityTheft.gov* or call 1-877-ID-THEFT (877-438-4338).

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may contact one of the three credit reporting agencies identified above. You may be required to provide information that identifies you including your full name, social security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. Depending on where you live, there should be no charge to request a security freeze or to remove a security freeze.

KROLL

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services [1] include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

HOW TO ACTIVATE YOUR IDENTITY MONITORING SERVICES

1. You must activate your identity monitoring services by March 31, 2022. Your Activation Code will not work after this date.
2. Visit **Enroll.krollmonitoring.com/redeem** to activate your identity monitoring services.
3. Provide Your Activation Code: **<<Enter Activation Code>>** and Your Verification ID: **<<Enter Verification ID>>**

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services [1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

---

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.