17679

Raymond A. Mason
School of Business
WILLIAM & MARY

FULL NAME
ADDRESS
CITY, ST ZIP

September 10, 2020

NOTICE OF DATA BREACH

Dear FULL NAME,

We take your privacy and security seriously at William & Mary and value the trust you place in us when you share your personal information. We wanted to make you aware of a data security incident involving Blackbaud, Inc., a vendor of William & Mary and the William & Mary Business School Foundation that provides data processing and hosting services. Blackbaud also provides similar services to thousands of universities and nonprofits worldwide.

What Happened

On July 16, 2020 Blackbaud notified us that it was the victim of a cyber-attack affecting the personal information of a limited number of students that were previously enrolled in the William & Mary Executive MBA program and that was associated with certain billing and accounts receivable activity performed by the Business School Foundation, including your personal information. On August 14, 2020, we were able to determine which individuals may have had personal information affected.

What Information Was Involved

The impacted information consisted of your name, address, and Social Security number that the William & Mary Business School Foundation keeps on Blackbaud's servers for its purposes and in supporting the needs of the university.

Please note that this billing and accounts receivable information was held in a different system from any donor engagement information that may have been affected by the incident and for which you may have received a separate communication. Such donor engagement information did not include any sensitive information, such as dates of birth, social security numbers, or financial data.

What We Are Doing

After we learned of this issue, we began a review. We understand that Blackbaud, law enforcement and third-party experts have investigated this incident, and that Blackbaud has hired a third-party firm to monitor for any misuse or public posting of the impacted dataset. We also understand that Blackbaud has taken steps to prevent this specific issue from happening again.

What You Can Do

We encourage you to remain vigilant in monitoring your account statements and credit reports for unusual activity. We also encourage you to enroll in the complimentary identity monitoring services we

are offering. The enclosed Reference Guide contains additional information about steps you can take to protect against unauthorized use of your personal information.

For More Information

We apologize for any concern or inconvenience this breach has caused. If you have any questions or concerns, please see contact us at blackbaudincident@wm.edu or by calling the Business School's Alumni Office at (757) 221-2874.

Thank you,

Ed Aractingi

Ed Aractingi
Chief Information Officer, William & Mary

Lawrence B. Pulley
Dean, Raymond A. Mason School of Business

Susan Rucker
CFO, William & Mary Business School Foundation

Reference Guide

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Enroll in Complimentary Identity Monitoring Services

To help protect your identity, we are offering a complimentary two year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by December 3, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **2JY746JS2**

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 toll free at (877) 890-9332 by December 3, 2010. Be prepared to provide engagement number DB13783 as proof of eligibility for the identity restoration services by Experian.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800 -525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

As of September 21, 2018, you have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of Massachusetts

Please also note that you have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.