WESTMINSTER
COLLEGE
1840 South 1300 East
Salt Lake City, UT 84105

December 28, 2018

##E3208-L01-0000046 0001 00000001 **********MIXED AADC 159
SAMPLE A SAMPLE - NON MA
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

Westminster College ("Westminster") values and respects your privacy, which is why we're writing to make you aware of a recent incident that may have involved your personal information.

What Happened

Westminster was the victim of a phishing attack in which an unauthorized third party gained access to the account of a Westminster employee. In investigating this attack, Westminster conducted an organization-wide audit and identified evidence of potential unauthorized access to 11 email accounts. Although Westminster has no evidence that an attacker used the information in those email boxes to commit any sort of fraud or identity theft, Westminster reviewed the documents in those email boxes to determine what personal information could potentially have been accessible. On November 30, 2018, we concluded our investigation and determined that your personal information may have been accessible in one of the affected email accounts. Thus, out of an abundance of caution, we're providing this notice to you. Westminster has no evidence that any other systems were affected or accessed, and there is no indication that there was any failure of Westminster's information security systems.

What Information Was Involved

The information potentially at risk may include your name, address, date of birth, Social Security Number, bank account number, credit card number, driver's license number, passport number, and/or protected health information.

0000046

What We Are Doing

Investigation. Westminster promptly had the affected users change their login credentials to ensure that the attacker's access was terminated. To ensure that an adequate investigation was conducted, we retained a forensic investigation firm to conduct an investigation regarding the nature of the incident, the scope of the affected information, and the potentially responsible parties.

Mitigation. Westminster has retained Experian to provide, at no cost to you, credit monitoring services. The details for opting in to these services are set forth below.

E3208-L01

Protection Against Further Harm. The attacker's access to the e-mail accounts has been terminated, and Westminster has redoubled its efforts to ensure the confidentiality of account access credentials. At this time, we're not aware of any further threat to the information via this phishing attack.

What You Can Do

Although we do not have any evidence that your information was misused as a result of this incident, you may be at risk. To help protect you, we have partnered with Experian to provide its IdentityWorks℠ product.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks℠ as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **March 31, 2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 451-6558. Be prepared to provide engagement number **DB10130** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

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

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.

Remain vigilant for any unauthorized use of your information. We suggest that you monitor your credit reports, which you can obtain for free from the three credit reporting agencies listed below. If you suspect incidents of identity theft, you should notify local law enforcement and/or your state attorney general.

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	Fraud Victim Asst. Div.
Atlanta, GA 30348	Allen, TX 75013	P.O. Box 6790
(800) 525-6285	(888) 397-3742	Fullerton, CA 92834
www.equifax.com	www.experian.com	(800) 680-7289
		www.transunion.com

You may also 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 ninety (90) days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

For More Information

If you have questions or concerns, please contact our toll free number, (888) 451-6558, between the hours of 9am-9pm Monday through Friday and Saturday-Sunday from 11am-8pm Eastern Standard. Additionally, for more information about avoiding identity theft, you can contact the Federal Trade Commission at 600 Pennsylvania Ave. N.W., Washington, D.C. 20580, 1-877-ID-THEFT, consumer.ftc.gov. Residents of Maryland may also obtain information about avoiding identity theft from the Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. Residents of North Carolina may also obtain information about avoiding identity theft from the North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov. Residents of Oregon may also obtain information about avoiding identity theft from the Oregon Office of the Attorney General at 1162 Court St. NE, Salem, OR, 97301-4096, 1-877-877-9392, https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/.

Sincerely,

Robert Allred
Chief Information Officer

0000046

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions