18249

THE UNIVERSITY OF MEMPHIS

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name 1>>:

The University of Memphis maintains personal information regarding its students, faculty and staff. The University considers this information to be highly confidential and maintains policies, procedures, and technologies to safeguard this information. Recently, the UofM determined that, notwithstanding our policies, procedures, and technologies, confidential personal information relating to you and others was accessible by an individual who obtained unauthorized access to a single University email account. Although the University has no indication the information was stolen, it was accessible in unencrypted format. Therefore, I am writing to advise you regarding this data security incident and to inform you about the steps the UofM has taken to secure the information as well as steps you may take in response to the incident.

Important Notice WHAT HAPPENED?

- On October 30, 2020, the University received a report of suspicious behavior related to email access and determined that one email account had been accessed without appropriate authorization. Immediate steps were taken on October 30, 2020, to secure the email account access. Law enforcement authorities were notified, and an investigation was launched on November 4, 2020, to determine if any personally identifiable information may have been involved. On November 11, 2020, the investigation determined that some confidential data for certain faculty and staff members were contained in the email account and were accessible by the unauthorized user. The UofM has identified you as one of the faculty or staff members whose information was accessible.

WHAT INFORMATION WAS INVOLVED?

- Inappropriate access to the email account was available October 23, 2020 through October 30, 2020;
- The data included individual names, social security numbers, addresses, and telephone numbers. The data were not encrypted.

CORRECTIVE ACTIONS

The University took immediate steps to contain and revoke the unauthorized access, and employees have been reminded of policies and procedures designed to protect confidential information. Annual IT Security Awareness Training for employees is on-going and additional technologies are being reviewed to strengthen compliance with data security policies and guidelines. The University has engaged with Epiq Monitoring Services to assist with this notice and offer services mentioned below.

WHAT WE ARE DOING.

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code **<<Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1- 855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft. This service includes access to an identity restoration specialist that provides assistance in the event that your identity is compromised.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

WHAT YOU CAN DO.

Fraud Alert Information

Whether or not you enroll in credit monitoring, we recommend that you place a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
www.equifax.com	www.transunion.com/fraud	www.experian.com
1-800-525-6285	1-800-680-7289	1-888-397-3742

Free Credit Report Information

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at 1-877-ID-THEFT (1-877- 438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC's website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "*Identity Theft - A Recovery Plan*".

Security Freeze Information

You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
http://transunion.com/freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

- Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.)
- Your Social Security Number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
- If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- Include applicable fee. Call or visit each of the credit reporting company websites listed above for information on fees for Security Freeze services. Forms of payment are check, money order, or credit card (American Express, Discover, MasterCard and Visa), or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

Within 5 business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if their child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security Number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

FOR MORE INFORMATION.

Frequently asked questions about this incident are located at https://www.memphis.edu/its/security/incidents.

We regret that this incident has occurred. Please be assured that the University of Memphis is taking steps to ensure that a breach of this nature will not happen in the future. If you have any further questions, you can call the University of Memphis incident response line at 855-914-4720 8am to 8pm Central Time, Monday through Friday (excluding US Holidays).

Sincerely,

Robert Jackson

Chief Information Officer