

RE: Notice of Data Breach

Dear Sir or Madam

The Office of Technology Services at the University of Baltimore, located at 1420 N Charles Street, Baltimore, MD 21202 is writing to notify your office of an incident that may affect the security of some personal information relating to one (1) Maryland resident. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, the University does not waive any rights or defenses it may have, including without limitation, any rights and defenses it may have regarding the applicability of Maryland law or the applicability of the Maryland data breach notification statute.

Nature of the Breach

On May 25, 2022, the Office of Technology Services of the University of Baltimore was notified that a file containing personal information of one individual was inadvertently e-mailed by an employee of the University to 8 email addresses not authorized to receive that file. Upon being notified that this accidental exposure happened, the University immediately instructed the individuals who received the file to delete it.

The information that may have been subject to unauthorized access include the individual's social security number, as well as the individual's bank account number and routing number. The University is not aware of any actual or attempted misuse of this information.

Notice to Maryland Residents

Beginning June 14, 2022, the University is sending written notice of this incident to the potentially affected individual. A copy of the written notice is attached.

Other Steps the University is Taking

Upon learning of the incident, the University's Computer Security Incident Response Team, together with the Office of Human Resources, undertook an investigation and review of the University's existing policies and procedures related to the handling of personal information. The University will implement additional safeguards to try to prevent a similar issue from recurring in the future following its investigation and review. The University is also providing the affected individual with information on how to place a fraud alert and security freeze on their credit file, information on protecting against fraud, the contact information for national consumer reporting agencies, information on how to obtain a free credit report, encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted to actual identity theft or fraud, and is also offering one-year of free credit monitoring through Experian.

A copy of the draft notification letter being sent to the individual potentially affected is enclosed with this letter. Should you have any questions regarding this notification or this security breach, please do not hesitate to contact us.

Edward Hodges

June 14, 2022

Notice of Data Breach

Dear _____:

The University of Baltimore is writing to alert you about a recent data security incident that involved some of your personal information. Although we have no reason to believe that your information was or will be misused, we take this incident seriously and want to inform you about what happened. We also want to provide resources to help you protect your personal information, including one year of credit monitoring should you decide to enroll as set forth below.

What Happened?

On May 25, 2022, the Office of Technology Services of the University of Baltimore was notified that a file containing your personal information was inadvertently e-mailed by an employee of the University to 8 email addresses not authorized to receive that file. Upon being notified that this accidental exposure happened, the University immediately instructed the individuals who received the file to delete it.

What Information Was Involved?

The information contained in the misdirected file included your name and social security number, as well as your bank account number and routing number. The University is not aware of any actual or attempted misuse of this information.

What Are We Doing In Response?

Upon learning that this incident occurred, the University of Baltimore Computer Security Incident Response Team, together with the Office of Human Resources, undertook an investigation and review of our existing policies and procedures relating to the handling of personal information. We will implement additional safeguards as appropriate to try to prevent something like this from happening again.

To help protect your identity, we are offering a complimentary **12-month** membership of Experian's® IdentityWorksSM. 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: 09/08/22** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: RCZBQMSVN**

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 at 877.288.8057 by **09/08/22**. Be prepared to provide engagement number **B054535** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR **12-MONTH 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.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 at [877.288.8057](tel:877.288.8057). 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 Identity Restoration support is available to you for **12 months** 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.

What Can You Do?

We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your account statements and credit reports for suspicious activity and reviewing the attached information under the caption, "Steps to Help Protect Your Information."

For More Information

We encourage you to review the information contained in this letter and take the steps recommended. We recognize that you may have questions that have not been addressed in this letter. If you have additional questions, please contact us at UB-CSIRT@ubalt.edu.

We regret any inconvenience or concern this incident may cause you and are available to answer your questions.

Sincerely,

University of Baltimore Computer Security Incident Response Team

Steps to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your 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 should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission ("FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting 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 also contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Fraud Alert: 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 one year. 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 www.annualcreditreport.com.

Security Freeze: You have the right to place a security freeze on your credit file. This will prevent new credit from being opened in your name without your express authorization. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the Federal Trade Commission or from your state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to your state Attorney General.

Federal Trade Commission (FTC): The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and, TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them as explained on their website. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

Maryland Office of the Attorney General: the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov .

Fair Credit Reporting Act (FCRA): Your rights under the FCRA include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies to correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit. www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf