



April 11, 2023

VIA E-MAIL (Idtheft@oag.state.md.us)

Re: Notice of Security Incident involving Boston University

Dear Attorney General Brown:

We write to you on behalf of Trustees of Boston University (the "University") to notify you of a recent security incident that affected the personal information of one Maryland resident.

The University detected a potential data breach event with respect to a compromised shared account used by the Metropolitan College (MET) Summer Term Program. The Information Security department was alerted to a potential anomalous activity of a compromised BU account, with the activity occurring potentially as far back as February 4, 2023. Boston University immediately began to review the situation, confirmed the account was compromised and subsequently identified the individuals whose personal information may have been affected.

Notice to Maryland Residents

The University intends to provide written notice of this incident to all affected individuals for whom we have current addresses in the State of Maryland, which includes one Maryland resident. A copy of the form of notification letter the University intends to send is attached. The University does not have any knowledge that the information of any party has been used for any unauthorized purpose. The compromised information may have included personal information provided during the application or enrollment process with the University's MET Summer Term program, including name, date of birth, social security number, and/or financial account number.

Other Steps Taken

Upon learning of this event, the password for the University account was immediately reset and multifactor authentication was enabled for the account. The University is further reviewing the security controls and practices within the affected department.

If you have any questions, please do not hesitate to contact me.

A handwritten signature in black ink, appearing to read "Martin G.", followed by a long horizontal line.

Associate General Counsel
Boston University
moppen@bu.edu

Enclosure

DATE

«First» «Last»

«Address1»

«Address11»

Notice of Data Breach

Dear «First»:

We are writing to inform you that Boston University has been actively investigating a data security incident that affected some students who applied for summer programs at Boston University Metropolitan College (the “MET College”). After an extensive review, we have determined that personally identifiable information you submitted to the MET College was stored in an email mailbox that was accessed by an unauthorized individual. We take the protection and proper use of your information very seriously and are providing this notice and a free 24-month membership in a credit monitoring service, Experian’s IdentityWorks, to help you protect your personal information.

What Happened?

On February 7th, Boston University detected a potential data breach event with a compromised shared account used by the Metropolitan College (MET) Summer Term Program. The Information Security department was alerted to the potential anomalous activity of a compromised Boston University email account belonging to the MET College Summer Term Program, with the activity occurring potentially as far back as February 4th. Boston University immediately began to review the situation, confirmed the account was compromised, and identified the individuals whose personal information may have been affected.

What Information Was Involved?

Affected information may include the personal information you provided during the application or enrollment process with the MET Summer Term program, including name, date of birth, social security number, and/or financial account number.

What We Are Doing.

Boston University is committed to safeguarding our community’s personal information. Upon learning of this event, the account’s password was immediately reset, multifactor authentication was enabled, and we are further reviewing the security controls and practices within the affected department.

What You Can Do.

At this time, Boston University does not have any knowledge that your information has been used for any unauthorized purpose. Therefore, this letter is *not* a notice that you are a victim of identity theft; it is a notice that there *may have been* unauthorized access to your information, not necessarily that it was accessed or has been used. Nevertheless, we are notifying you as required by state law and in an abundance of caution.

It is a good idea to continue to monitor your credit card and financial account statements. Therefore, the University is making available to you a free 24-month membership in a credit monitoring service, Single Bureau Credit Monitoring, which will provide you with alerts of key changes and suspicious activities on your credit reports and proactive fraud assistance. You must enroll by June 21, 2023. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Single Bureau Credit Monitoring is free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Single Bureau Credit Monitoring, including instructions on how to activate your complimentary 24-month membership, please review the enclosed document.

You may also take advantage of the free annual credit report available from each credit reporting agency by visiting www.annualcreditreport.com. You have the right to obtain such a free report annually, from each of the three major credit reporting bureaus. If you detect any unauthorized or suspicious activity in any of your accounts, contact the issuing company immediately. If you believe it may be related to this event, please contact us at BUInfoSec@bu.edu, referring to case #20230100374.

To learn more about steps you can take to protect yourself from identity theft, you may contact or visit the websites for the Federal Trade Commission and your state's Office of the Attorney General. The websites, telephone numbers, and addresses of these agencies are included in this notice.

Under the circumstances, we felt there was no need to file a police report except where specifically required by applicable state law to do so. However, if you are victim of identity theft—meaning that your personal identifying information was used to pose as you, harass you, or obtain identification containing your personal information or anything else of value—you have the right to file your own police report and obtain a copy of that report.

If you find that your information is being used without your authorization, contact your local police department.

Consumers may choose to place a security freeze on their credit reports. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. Details on how to request a security freeze or a fraud alert are attached to this letter.



For More Information.

Boston University takes privacy and information security very seriously and is taking steps to prevent any similar events in the future. We regret that your information may have been subject to unauthorized access and any inconvenience or concern caused by this incident. Should you have further questions about this matter, please call 617-358-8500 and refer to case #20230100374.

Sincerely,

Eric Jacobsen
Assistant Vice President and CISO, BU Information Security

Enclosure:

*Information about Identity Theft Prevention
Experian's® IdentityWorks® Alert Enrollment Instructions
Resources and Contact Information by State*

Information about Identity Theft Prevention

Credit Reports

To monitor the ongoing health of your credit, you should periodically review your credit reports. The Fair Credit Reporting Act (FCRA) requires each of the nationwide consumer reporting agencies – Equifax, Experian, and TransUnion – to provide you with a free copy of your credit report, at your request, once every 12 months.

You may obtain your free credit reports online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com). You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 740241, Atlanta, Georgia 30348, 1-800-685-1111, www.equifax.com

Experian, P.O. Box 2104, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-680-7289, www.transunion.com

Fraud Alerts

When a fraud alert is in place, potential creditors must use what the law refers to as “reasonable policies and procedures” to verify your identity before issuing credit in your name. However, a fraud alert will not prevent the opening of new accounts in your name that do not require a credit check.

You may request a fraud alert by calling or writing any one of the three credit reporting agencies listed above. Some of them also allow you to place a fraud alert online:

https://www.experian.com/consumer/cac/FCRegistration.do?alertType=INITIAL_ALERT

[https://www.alerts.equifax.com/AutoFraud Online/jsp/fraudAlert.jsp](https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp)

You need contact only one of the above companies; whichever one you call will alert the others.

You will need to provide them with your name, address, social security number and birth date.

When you request an alert, the bureaus are required to provide you a copy of your credit report free of charge. Request your free report and review it thoroughly. If you detect any fraudulent activity, you should immediately contact the agency issuing the account.

Security Freeze

You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax, Experian, and TransUnion by certified mail, overnight mail, or regular stamped mail at the addresses above.

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. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard. American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Internal Revenue Service

If you believe your tax records may be affected by identity theft you may alert the Internal Revenue Service. Information about that process is available from the IRS:

<http://www.irs.gov/privacy/article/0,,id=186436,00.html>

More information on identity theft is available from the **Federal Trade Commission (FTC)**:

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Avenue, NW, Washington, DC 20580,

1-877-IDTHEFT (438-4338)

TDD: 1-202-326-2502

www.ftc.gov/idtheft

To help protect your identity, we are offering a **complimentary** two-year membership of Experian's® IdentityWorks®. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Now in Three Easy Steps

1. ENSURE That You Enroll By: **June 21, 2023** (Your code will not work after this date.)
2. VISIT the **IdentityWorks Web Site to enroll:**
<https://www.experianidworks.com/3bcredit>
3. PROVIDE Your Activation Code: **«Code»**

If you have questions or need an alternative to enrolling online, please call 877-288-8057.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH IDENTITYWORKS MEMBERSHIP:

A credit card is not required for enrollment.

Once your IdentityWorks membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
- **\$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

Once your enrollment in IdentityWorks is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-2

Resources and Contact Information by State

You can obtain more information about fraud alerts, credit freezes, and other steps you can take to avoid identity theft by contacting the government agencies or one of the national credit reporting agencies listed below.

Contact Information for the Three Nationwide Credit Reporting Agencies:

Equifax, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com/personal/credit-report-services, 1 (800) 685-1111

Experian, P.O. Box 2002, Allen, TX 75013, www.experian.com/help, 1 (888) 397-3742

TransUnion, P.O. Box 2000, Chester, PA 19022, www.transunion.com/credit-help, 1 (888) 909-8872

Contact Information for Relevant Government Agencies:

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

Alabama Office of the Attorney General, 501 Washington Avenue, Montgomery, AL 36104, www.alabamaag.gov, 1 (800) 626-7676

Arkansas Office of the Attorney General, 323 Center Street, Suite 200, Little Rock, Arkansas 72201, www.arkansasag.gov, 1 (800) 482-8982

California Office of the Attorney General, P.O. Box 944255, Sacramento, CA 94244, www.oag.ca.gov, 1 (800) 952-5225

Florida Office of the Attorney General, 111 West Madison Street, Tallahassee, FL 32399, www.oppaga.fl.gov or www.myfloridalegal.com, 1 (850) 414-3990

Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1 (888) 743-0023

Massachusetts Office of the Attorney General, One Ashburton Place, Boston, MA 02108, www.mass.gov/orgs/office-of-the-attorney-general, 1 (800) 626-7676

New Jersey Office of the Attorney General, 25 Market Street, P.O. Box 081, Trenton, NJ 08625, www.njoag.gov, 1 (609) 984-5828

New York Office of the Attorney General, The Capitol, Albany, NY 12224, www.ag.ny.gov, 1 (800) 771-7755

Nevada Office of the Attorney General, 100 North Carson Street, Carson City, NV 89701, www.ag.nv.gov, 1 (888) 434-9989

Puerto Rico Department of Consumer Affairs, Ave. José De Diego, Pda. 22, Minillas Government Center, North Tower Building, 8th Floor, San Juan, 00940, www.daco.pr.gov, 1 (787) 722-7555

Texas Office of the Attorney General, P.O. Box 12548, Austin, TX 78711, www.texasattorneygeneral.gov, 1 (800) 621-0508

Wisconsin Office of the Attorney General, P.O. Box 7857, Madison, WI 53707, www.doj.state.wi.us, 1 (608) 266-1221