



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

November 5, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Worcester Polytechnic Institute (“WPI”) located at 100 Institute Rd, Worcester, MA 01609, and are writing to notify your office of an incident that may affect the security of certain personal information relating to seventy-two (72) Maryland residents. By providing this notice, WPI does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 18, 2024, WPI learned that a software application share intended to have restricted staff access only inadvertently allowed other WPI users to access it. The access granted the WPI community only an ability to view some student personal information. A WPI student inadvertently discovered the broader-than-intended access and self-reported the inadvertent access to WPI. WPI quickly applied access restrictions to the share. WPI then launched an internal investigation and engaged third-party specialists to validate independently that no other connection occurred. In parallel, WPI reviewed internally the accessible data to identify the individuals whose information resided in it at the time of the inadvertent access. WPI completed that review on October 11, 2024, and confirmed that some personally identifiable information was present. On October 15, 2024, the third-party specialists confirmed that no connection outside of the WPI community occurred. The information subject to unauthorized access varies by individual and may include name and Social Security number.

Notice to Maryland Residents

On or about November 5, 2024, WPI provided written notice of this event to seventy-two (72) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, WPI moved quickly to investigate and respond to the event, assess the security of WPI's software application share, and identify individuals whose information was accessed inadvertently. WPI is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose Social Security numbers were accessed inadvertently, at no cost to those individuals.

Additionally, WPI is providing impacted individuals with guidance on how to better protect against identity theft and fraud. WPI is providing individuals with information on how to place fraud alerts and credit freezes on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

WPI is providing written notice of this event to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2303.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Lynda Jensen".

Lynda Jensen of
MULLEN COUGHLIN LLC

EXHIBIT A



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

Enrollment Code: <<Activation Code>>

Or Visit:

<https://www.experianidworks.com/credit>

<<Date>>

NOTICE OF <<VARIABLE DATA 1>>

Dear <<Full Name>>:

Worcester Polytechnic Institute ("WPI") writes to notify you of an event that may affect the privacy of some of your information. This letter provides details of the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so.

What Happened. On September 18, 2024, WPI learned that a software application share intended to have restricted staff access only inadvertently allowed other WPI users to access it. The access granted the WPI community only an ability to view some student personal information. A WPI student inadvertently discovered the broader-than-intended access and self-reported the inadvertent access to WPI. We quickly applied access restrictions to the share. We then launched an internal investigation and engaged third-party specialists to validate independently that no other connection occurred. In parallel, we reviewed internally the accessible data to identify the individuals whose information resided in it at the time of the inadvertent access. We completed that review on October 11, 2024, and confirmed that some of your information was present. On October 15, 2024, the third-party specialists confirmed that no connection outside of the WPI community occurred.

What Information Was Involved. Our investigation determined that your name and Social Security number resided in the data accessible to the WPI student. We have no indication that your information was used to commit identity theft or fraud and are providing this notice out of an abundance of caution.

What We Are Doing. Data privacy and security are among WPI's highest priorities, and there are measures in place to protect the information in our care. Upon learning of the inadvertent access to the software application share, we investigated internally and with the assistance of third-party specialists to confirm the scope of this event. The investigation and response included confirming the security of our share, reviewing the contents of accessible data to determine the individuals to which any sensitive data in it related, and notifying the identified individuals. Although we have measures in place to protect information in our care, as part of our ongoing commitment to the privacy of information, we regularly review our policies, procedures, and processes related to the storage and access of personal information to limit the likelihood that similar events will occur in the future. We will notify applicable regulatory authorities, where necessary.

This event occurred when a WPI student inadvertently viewed data without authorization. Although no criminal activity occurred or is suspected, as an added precaution, we are offering you access to <<CM Duration>>-months of complimentary access to credit monitoring services through Experian at no cost to you. For more information, including how to enroll to receive the offered services, please follow the instructions in the attached **Steps You Can Take to Help Protect Your Personal Information**. Although WPI is covering the cost of the credit monitoring services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included in this letter.

What You Can Do. We have not identified a potential risk of identity fraud or theft as a result of this event. Steps you may wish to take in response to this event are a personal decision. As a matter of good practice, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and by monitoring your credit reports for suspicious activity. You should promptly report any suspicious behavior to your financial institution/credit or debit card and report any activity indicative of identity theft or fraud to law enforcement. Please also review the enclosed ***Steps You Can Take to Help Protect Your Personal Information*** for additional information and resources. You also can enroll to receive the complimentary credit monitoring services that we are offering.

For More Information. We understand you may have questions about the event that are not addressed in this letter. If you have questions, or need assistance, please call 855-278-0561, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding U.S. holidays. You may also write directly to us at: Worcester Polytechnic Institute at inquiries@wpi.edu.

Sincerely,

Worcester Polytechnic Institute

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for <<CM Duration>> months.

If you believe there was fraudulent use of your information as a result of this event 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 from the date of the incident (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 Identity Restoration is available to you for <<CM Duration>> 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.

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 <<CM Duration>>-month 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** <<Enrollment Deadline>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: <<Activation Code>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this event, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057 by <<Enrollment Deadline>>. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the Identity Restoration services by Experian.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.