

Jim Giszczak
Direct Dial: 313.407.4049
E-mail: jgiszczak@mcdonaldhopkins.com

November 10, 2022

VIA EMAIL fldthefi@pas.state.md.us

Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202



Re: Lehigh University– Data Security Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Lehigh University (“Lehigh”). I am writing to provide notification of an incident at Lehigh that may affect the security of personal information of approximately one (1) Maryland resident. Lehigh’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Lehigh does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about November 1, 2022, an unauthorized individual broke into a locked box which contained a limited number of human resource files. These files were physical, paper documents, not electronic files. Upon learning of this issue, Lehigh University immediately commenced a prompt and thorough investigation. As part of its investigation, Lehigh University has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive investigation into the incident, Lehigh University discovered on November 2, 2022 that certain human resource files were stolen from a locked box on campus by an unauthorized individual(s). The files contained the personal information of one (1) Maryland resident, including name, Social Security number, and passport number.

Lehigh is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Lehigh wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Lehigh is providing the affected residents with written notification of this incident commencing on or about November 10, 2022 in substantially the same form as the letter attached hereto. Lehigh is offering the affected resident whose Social Security number was affected complimentary one-year membership with a credit monitoring service. Lehigh will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Lehigh will advise the affected resident about

November 10, 2022

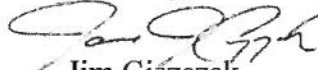
Page 2

the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Lehigh, protecting the privacy of personal information is a top priority. Lehigh is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Lehigh continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (313) 407-4049 or jgiszczak@mcdonaldhopkins.com.

Sincerely,



Jim Giszczak

Encl.



LEHIGH
UNIVERSITY

306 South New Street, Suite 451
Bethlehem, PA 18015

Office:

e-mail:



To Enroll, Please Call:

Or Visit:

Enrollment Code:

Dear ,

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Lehigh University ("Lehigh"). We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

On or about November 1, 2022, an unauthorized individual broke into a secured, locked box which contained a limited number of physical files.

What We Are Doing

Upon discovering the incident, we commenced an immediate and thorough investigation and alerted law enforcement. As part of our investigation, we worked to identify what personal information, if any, might have been present in the locked box.

What Information Was Involved

After an extensive investigation into the incident, we discovered that one or more of the files taken by the unauthorized party contained

What You Can Do

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Nevertheless, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Please note the deadline to enroll is **April 1, 2023**. This letter also provides other precautionary measures

you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

At Lehigh, protecting the privacy of personal information is a top priority. We are committed to maintaining the privacy of personal information in our control and we continue to take many precautions to safeguard it.

Please review the attached Frequently Asked Questions (FAQ) document for additional information. If you have a question that is not addressed in the FAQ, please contact [REDACTED] at [REDACTED].

Sincerely

[REDACTED]

[REDACTED]

Controller

Lehigh University Frequently Asked Questions (FAQ)

(1) What happened?

On November 9, 2022, Lehigh University notified certain individuals about a security incident.

On November 1, 2022, the Lehigh University discovered that an unauthorized party broke into a locked box which contained a limited number of physical files. The files were taken by the unauthorized person. Upon detecting the incident, we commenced an immediate and thorough investigation and alerted law enforcement. As part of its investigation, we worked to identify what personal information, if any, might have been present in the locked box.

We have no evidence that any information was misused. However, out of an abundance of caution, we wanted to inform you of the incident.

(2) Who is affected by this incident?

A limited number of new hires were affected by this incident.

(3) Why was there a delay in notification of this incident?

There was no delay. Upon detecting the incident, Lehigh University immediately commenced a prompt and thorough investigation to determine the scope and impact of the intrusion. Once it was determined who was impacted, and what information of theirs was impacted, the individuals were provided notice.

(4) Is Lehigh University providing credit monitoring services?

Lehigh University is offering credit monitoring through IDX for individuals whose Social Security numbers were involved in this incident.

(5) Can Lehigh University just register me in the credit monitoring product?

Unfortunately, Lehigh University cannot register for you. You must enroll yourself online (or over the phone) using the Activation Code in your notice letter if you received one.

(6) How long do I have to enroll in the credit monitoring product?

If you received credit monitoring services, you can sign up for this service anytime between now and April 1, 2023 using the Activation Code listed in your notification letter.

(7) Has the unauthorized individual been identified or caught?

Lehigh University is not aware that the unauthorized individual has been identified or caught. However, law enforcement's investigation is ongoing. Lehigh University's primary focus remains on supporting those individuals who were impacted by this incident.

(8) Will we receive any additional information or update?

If a further update is warranted, Lehigh University will provide one accordingly.

(9) What is a fraud alert?

A fraud alert tells creditors to contact you personally before they open any new accounts.

(10) How do I place a fraud alert on my account?

In order to place a fraud alert, you will need to call any one of the three major credit bureaus (as soon as one credit bureau confirms your fraud alert, they will notify the others to place fraud alerts). Alternatively, you may file the Fraud Alert online. Here is a link to the Experian fraud alert home page: <https://www.experian.com/fraud/center.html>

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

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

TransUnion
P.O. Box 2000
Chester, PA 19022
www.transunion.com
1-800-680-7289

(11) How long does a fraud alert last?

An initial fraud alert lasts one year and it is free.

(12) Will a fraud alert stop me from using my credit cards?

No. A fraud alert will not stop you from using your credit cards or other accounts.

(13) Can I still apply for a credit card after I place a fraud alert on my credit report?

Yes, but the verification process may be more cumbersome. Potential creditors will receive a message alerting them to the possibility of fraud and that creditors should re-verify the identity of a person applying for credit.

(14) How do I place a Security Freeze on my credit files and how much does it cost?

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no cost to you. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

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

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

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19022
www.transunion.com/securityfreeze
1-800-680-7289

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

(15) What should I do if I find suspicious activity on my credit reports or have reason to believe my information is being misused?

Promptly call your local law enforcement agency and file a police report. Get a copy of the police report, as many creditors will want the information it contains to absolve you of fraudulent debts. You may also file a complaint with the FTC at www.ftc.gov/idtheft or reach the FTC at 1-877-IDTHEFT (1-877-438-4338) or 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

(16) When I called to place a fraud alert, they asked for my Social Security number. Is this ok?

Yes. The credit bureaus will indeed ask for your Social Security number and other personal information to verify your identity and avoid sending any credit report or correspondence to the wrong individual. However, Lehigh University cautions against you providing any information to any entity or person *contacting you directly* asking for your personal information.

(17) How do I obtain a free credit report?

Under federal law, you are entitled to one free credit report every 12 months from each of the three major credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

(18) I lost my notification. Can you provide a new one to me?

Yes. Please confirm your name and address and Lehigh University will ensure that you receive another notification if you are confirmed to be potentially impacted.

(19) I have experienced fraud on my payment card. What do I do?

If you see a fraudulent charge on your payment card, you should immediately contact the bank, credit union or other financial institution that issued your card. The phone number to call can be found on the back of the card. If reported promptly, major credit card companies typically guarantee cardholders will not be responsible for fraudulent charges.

(20) Is this letter legitimate? Is it a scam?

I can assure you the letter is legitimate. Safeguarding information is a top priority for Lehigh University. Lehigh University wants to make you aware of the situation and provide you with guidance on how you can protect yourself.

(21) Do I have any legal recourse?

Unfortunately, Lehigh University is not in a position to provide any legal advice related to the incident.

(22) Has the unauthorized individual been identified or caught?

Lehigh University is not aware that the unauthorized individual has been identified or caught. However, law enforcement's investigation remains ongoing. Lehigh University's primary focus remains on supporting those individuals who were impacted by this incident.

(23) I have additional questions that cannot be answered. What should I do?

If you have a question that is not addressed in this FAQ, please contact our Associate Controller at (610) 758-3177.