



Maria Efaplatidis
77 Water Street, Suite 2100
New York, NY 10005
Maria.Efaplatidis@lewisbrisbois.com
Direct: 212.232.1366

February 23, 2022

VIA EMAIL

Attorney General Brian Frosh
Maryland Attorney General's Office
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: ldtheft@oag.state.md.us

Re: **Notice of Data Security Incident**

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Creighton University ("Creighton") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute.

1. Nature of the Incident

Creighton is a private university located in Omaha, Nebraska.

On December 30, 2021, Creighton learned that an unauthorized user may have accessed Creighton's NEST system. NEST is the university's student portal that contains student data including transcripts, enrollment records, and direct deposit information for student aid. Upon learning of the unauthorized activity in NEST accounts, Creighton immediately launched an investigation. Creighton engaged a digital forensics firm to assist with the investigation and to determine whether personal information may have been accessed or compromised. Creighton also sent a message to all those whose NEST accounts may have been impacted, notifying users to change their login credentials and confirm that the information in their NEST accounts was accurate. On January 24, 2022, Creighton identified all users whose information may have been impacted by this unauthorized access.

2. Type of Information and Number of Maryland Residents Involved

The incident involved personal information for two (2) Maryland residents. The information involved in the incident may include name, date of birth, Social Security number, and financial account number.

Creighton will notify affected individuals via first class U.S. mail on February 24, 2022. A sample copy of the notification letter is included with this correspondence.

3. Measures Taken to Address the Incident

Creighton has taken the steps outlined above in response to this incident and made alterations to its cyber environment to help prevent similar incidents from occurring in the future. In addition, Creighton is providing impacted individuals with information about steps they can take to help protect their personal information. Creighton is also offering credit monitoring and identity protection services at no cost through IDX, which will help individuals resolve issues if their identity is compromised due to this incident.

4. Contact Information

Creighton remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 212.232.1366 or Maria.Efaplatidis@lewisbrisbois.com.

Sincerely,

A handwritten signature in dark ink, appearing to read 'MEF', with a long horizontal flourish extending to the right.

Maria Efaplatidis of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Enclosure: Sample Notification Letter

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 24, 2022

Re: Notice of <<Variable Data 1>>

Dear <<First Name>> <<Last Name>>,

At the Creighton University ("Creighton"), we take the privacy and security of your information very seriously. We are notifying you of a recent data security incident that may have involved some of your personal information and informing you about steps you can take to help protect your personal information.

What Happened? On December 30, 2021, Creighton learned that an unauthorized user may have accessed Creighton's NEST system. Upon learning of the unauthorized activity, we immediately launched an investigation. We engaged a digital forensics firm to assist with the investigation and determine whether personal information may have been accessed or compromised. We also sent a message to all those whose NEST accounts may have been impacted, notifying users to change their login credentials and confirm that the information in their NEST accounts was accurate. On January 24, 2022, Creighton identified all users whose information may have been impacted by this unauthorized access.

What Information Was Involved? Creighton completed a comprehensive review of the data that could have been accessed by the unauthorized actor and on January 4, 2022, determined that an unauthorized actor accessed your Creighton NEST account. The personal information that may have been accessed includes your name in combination with a Social Security number, date of birth, and/or financial account number.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also implemented enhanced security measures to prevent similar incidents in the future. In addition, we are providing you with information about steps you can take to help protect your personal information and offering free credit monitoring and identity protection services for 12 months through IDX. We offer you this service out of an abundance of caution.

What You Can Do: You can follow the recommendations included with this letter to protect your personal information. We strongly encourage you to enroll in the credit monitoring and identity protection services through IDX. To enroll, visit <https://app.idx.us/account-creation/protect> or call 1-800-939-4170 and provide the following enrollment code: <<Enrollment Code>>. Note that to receive credit monitoring services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing the services is included with this letter. You must enroll by May 24, 2022. If you have questions or need assistance, please call IDX at 1-800-939-4170.

For More Information: If you have any questions about this letter, please call 1-800-939-4170 between the hours of 8 a.m. to 8 p.m. Central Time. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this situation may cause you.

Sincerely,

A handwritten signature in cursive script, reading "Andrea M. Jahn". The signature is written in dark ink and is positioned above the printed name.

Andrea M. Jahn, J.D.
Associate General Counsel & University Privacy Officer
Creighton University

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing 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 also should 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 <http://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 also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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, 1-800-916-8800, 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 at least 90 days. 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 <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. 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. 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 FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Attorney General in your state and to the FTC at the following address:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.
- *New York Attorney General*, Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433
- *Maryland Attorney General*, 200 St. Paul Place, Baltimore, MD 21202, oag.state.md.us, 1-888-743-0023

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.