



Laura K. Funk
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Laura.Funk@lewisbrisbois.com
Direct: 972.942.5696

July 15, 2022

Via Electronic Mail

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Incident Notification
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents National University System ("NUS"), which is an affiliation of three accredited nonprofit universities, including National University (NU), Northcentral University (NCU), and City University of Seattle (CityU), in connection with a recent data security incident described in greater detail below.

1. Nature of the Security Incident

On May 26, 2022, NUS became aware of unusual network activity at NCU and subsequently discovered that NCU had been a victim of a data encryption event. NCU immediately took steps to secure the network and launched an investigation. In connection therewith, NUS engaged a leading, independent digital forensics and incident response firm to determine what happened and whether any sensitive information, including protected personal and student information, was affected as a result. The investigation determined that this incident was isolated to a limited number of servers, some of which contained student personal information. Thereafter, NUS worked to identify address information for the impacted individuals and prepared notification materials.

2. Type of Information and Number of Maryland Residents Involved

A total of forty-four (44) residents of Maryland were notified about this incident. The investigation determined that names, addresses, and financial aid information, including

Social Security numbers, may have been accessed or acquired without authorization for these residents.

Affected individuals received a letter notifying them of the incident, offering complimentary identity protection services, and providing additional steps they can take to protect their personal information. On July 15, 2022, the notification letters were sent via USPS First-Class Mail to all potentially impacted individuals.

3. Measures Taken to Address the Incident

Upon learning of this incident, NCU took steps to secure its environment. Additionally, NUS engaged a computer forensics firm to conduct an investigation into the incident. Finally, NCU has notified the potentially impacted individuals and provided them with information about steps they can take to help protect their personal information as well as offering complimentary identity protection services, 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

4. Contact Information

NUS is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact me by telephone at 972.942.5696 or via email at Laura.Funk@lewisbrisbois.com.

Sincerely,



Laura K. Funk of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LKF/sj

Encl: Sample Notification Letter



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

To Enroll, Please Call:
877.288.8057
Or Visit:
<https://experianidworks.com/3bcredit>
Enrollment Code: <<Account Code>>

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data <<Variable Header>>

Dear <<Name 1>>,

We are writing to inform you of a data security incident that involved your personal information. At Northcentral University (NCU), we take the privacy and security of student information very seriously. This is why we are notifying you of the incident, offering you credit monitoring and identity monitoring services, and informing you about steps you can take to help protect your personal information.

What Happened. On May 26, 2022, NCU became aware of unusual network activity in our environment. NCU immediately took steps to secure the network and launched an investigation. We also engaged a leading, independent digital forensics and incident response firm to determine what happened and whether any sensitive information, including protected personal and student information, was affected. As a result of the investigation, NCU identified that a small subset of student financial aid award information may have been acquired without authorization. Following a thorough review of the affected files, on June 21, 2022, we confirmed that your information was included.

What Information Was Involved. The information involved included your name, address, Social Security number, and student ID number.

What Are We Doing. As soon as we discovered the incident, we took the steps described above. In addition, we are offering you information about steps you can take to help protect your personal information, including free identity monitoring and recovery services for <<CM Length>> months through Experian's® IdentityWorksSM. These services include: tri-bureau credit monitoring, fraud alerts, and \$1,000,000 in identity theft insurance. With this protection, Experian will help you to resolve issues if your identity is compromised.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We also strongly encourage you to enroll in the monitoring services we are offering through Experian. To enroll, please visit <https://www.experianidworks.com/3bcredit> or call 877.288.8057 and provide the enrollment code listed at the top of this letter. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian. Please note that the deadline to enroll is <<Enrollment Deadline>>.

For More Information: If you have any questions about this letter, please call 1-844-997-2192 between 9am to 9pm Eastern Time from Monday to Friday. Representatives are fully versed in this incident and available to answer your questions. The security of your information is a top priority at Northcentral University, and we are committed to safeguarding your data. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Ian Cooper
Senior Vice President, Operations
Northcentral University

Steps You Can Take to 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 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 1-877-322-8228, 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 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
1-800-916-8800
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 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 <http://www.annualcreditreport.com>.

Security Freeze: 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 FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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 <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.