



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

RECEIVED  
JAN 3 2020  
CONSUMER PROTECTION

Michael J. Bonner  
Office: (267) 930-4815  
Fax: (267) 930-4771  
Email: mbonner@mullen.law

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

December 30, 2019

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent North Park University (“North Park”), located at 3225 West Foster Ave, Chicago, IL 60625, and are writing to notify your Office of an incident that may affect the security of some personal information relating to approximately six (6) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, North Park does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On September 23, 2019, North Park determined that an unknown actor had access to a single employee email account. Following discovery of unusual activity related to this email account, North Park immediately changed the account credentials and launched an investigation, with the assistance of a third-party computer forensics expert. The investigation determined that the email account was accessible on August 8, 2019 and September 5, 2019. Unfortunately, the investigation was not able to determine which emails, if any, were actually accessed or viewed.

North Park conducted a thorough manual and programmatic review to determine what information was contained in the email account and to whom the information related. On October 25, 2019, North Park confirmed the identities of individual who may have had information accessible in the email account. North Park then promptly reviewed their files to ascertain address information for the impacted individuals.

The information that could have been subject to unauthorized access includes name and Social Security number.

### **Notice to New Hampshire Residents**

On or about December 30, 2019, North Park provided written notice of this incident to affected individuals, which includes approximately six (6) New Hampshire 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 incident, North Park moved quickly to investigate and respond to the incident, assess the security of North Park systems, and notify potentially affected individuals. North Park is also working to implement additional safeguards and training to its employees. North Park is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, North Park is providing impacted individuals with guidance on how to better protect against identity theft and fraud. North Park is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against fraud, 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.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4815.

Very truly yours,



Michael J. Bonner of  
MULLEN COUGHLIN LLC

# EXHIBIT A



**NORTH PARK  
UNIVERSITY**  
CHICAGO

<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
 <<address\_1>>  
 <<address\_2>>  
 <<city>>, <<state\_province>> <<postal\_code>>  
 <<country >>

**RE: Notice of Data Breach**

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

North Park University (“North Park”) recently learned of unusual activity related to an employee email account. We write to provide you with information on the incident, the steps North Park is taking in response, and steps you may take to better protect your information, should you feel it is appropriate.

**What Happened?** On September 23, 2019, North Park determined that an unknown actor had access to a single employee email account. Following discovery of unusual activity related to this email account, North Park immediately changed the account credentials and launched an investigation, with the assistance of a third-party computer forensics expert. The investigation determined that the email account was accessed on August 8, 2019 and September 5, 2019. Unfortunately, the investigation was not able to determine which emails, if any, were actually accessed or viewed.

North Park undertook a comprehensive review of the email account to identify those who may have personal information accessible within the email account. Although, to date, we are unaware of any actual or attempted misuse of your personal information, we are notifying you in an abundance of caution because your information was present in the impacted email account at the time of the incident.

**What Information Was Involved?** The investigation confirmed the information present within the email account at the time of the incident included your <<b2b\_text\_1(Impacted Data)>><<b2b\_text\_2(Impacted Data)>>.

**What is North Park Doing.** We take the security of personal information in our care very seriously. Upon learning of this event, we promptly notified the relevant email account user, changed the email account credentials, and confirmed the security of other email accounts and systems. North Park has established security measures in place to protect data in our care. We are taking additional steps to enhance our data security including implementing increased security measures for account access such as multi-factor authentication and additional employee training. We are also notifying relevant state and federal regulators.

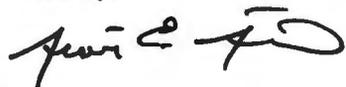
While to date, we have no evidence of actual or attempted misuse of your personal information as a result of this incident, out of an abundance of caution we are providing you access to 12 months of identity monitoring services through Kroll, at no cost to you. Information on how to activate these services may be found in the enclosed “Steps You Can Take to Help Protect Your Information.”

**What Can You Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You may review the information contained in enclosed “Steps You Can Take to Help Protect Your Information” for guidance on how to protect your information. You may also activate to receive the identity monitoring services we are making available to you as we are unable to activate these services on your behalf.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at [1-773-777-7777](tel:1-773-777-7777) which may be reached Monday through Friday, 8:00 a.m. to 5:30p.m., CT. You may also write to us at 3225 West Foster Ave., Chicago, IL 60625.

North Park takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in black ink, appearing to read "Scott Stenmark". The signature is written in a cursive style with a large, stylized initial "S".

Scott Stenmark  
Vice President for Finance and Administration  
North Park University

## **Steps You Can Take to Help Protect Your Information**

### **Activate Identity Monitoring**

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

### **Monitor Accounts**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

## **Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, [www.oag.state.md.us](http://www.oag.state.md.us).

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**For Rhode Island Residents**, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. [There are XX Rhode Island residents impacted by this incident.](#)

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

**For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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.



## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You've been provided with access to the following services<sup>1</sup> from Kroll:

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and 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.