NORTH HIGHLAND

September 28, 2022

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

RE: Follow-Up Notice Concerning Security Breach

To Whom It May Concern:

We are writing to provide you with a follow-up notice regarding an incident for which North Highland Company LLC, North Highland ESOP Holdings, Inc., and The North Highland Holding Company LLC (together, "North Highland" or "we") previously provided a notice. A copy of our previous notification is included herein. We have been identifying potentially impacted individuals in waves as we have been able to identify those individuals and their contact information. We notified current employees on July 8, 2022. On July 27, 2022 and August 10, 2022, we notified former employees dating back to approximately 2014 and dependent and beneficiaries of current and former employees that were designated in our benefits-related systems.

We have now completed our investigation. We found an additional 5 residents of New Hampshire since our last notice, resulting in a total number of 11 individuals affected in New Hampshire for this incident. We have notified the additional 5 residents of New Hampshire on August 10, 2022 and September 23, 2022. The sample breach letter sent to all additional residents is substantively the same as the sample notice we previously provided. A copy of the sample breach letter sent to additional residents is included herein.

Please do not hesitate to contact me if you have any questions.

Sincerely,

Patrick Ray
General Counsel
The North Highland Company, LLC
Patrick.Ray@northhighland.com
404.975.6602

July 27, 2022

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

RE: Notice Concerning Security Breach

To Whom It May Concern:

We are writing to notify you that North Highland Company LLC, North Highland ESOP Holdings, Inc., and The North Highland Holding Company LLC (together, "North Highland" or "we") have experienced a security incident. On June 6, 2022, North Highland discovered that it had been the victim of a ransomware attack. The attack encrypted a portion of our computer systems, rendering those systems temporarily unavailable. On the same day, North Highland began taking actions to stop the attack and initiated an investigation. We also engaged third-party cybersecurity experts to assist with our investigation and response efforts. We initiated a number of technical remediation efforts, including new password requirements for all employees.

On June 28, 2022, we determined that the incident affected the personal data of current employees and at least some former employees, including: names, national insurance numbers, social security numbers, identity numbers, tax numbers, addresses, bank account numbers and other payroll information, personal phone and email addresses, dates of birth, benefits information, background check and employment screening information, performance related records, medical related information employees may have provided to us, such as in connection with leave requests or an accommodation, and other employment-related information.

Our investigation has also confirmed that personal information of at least some beneficiaries and dependents of North Highland employees and former employees had been exfiltrated, including: dependent and beneficiary names, social security numbers, identity numbers, addresses, dates of birth, and other benefits-related information.

We have since determined that personal information pertaining to at least 6 employees and former employees and their dependents and beneficiaries from New Hampshire were or may have been impacted. We notified current employees on July 8, 2022 (none of whom were New Hampshire residents). On July 27, 2022, we notified former employees dating back to approximately 2014 and dependent and beneficiaries of current and former employees that were designated in our benefits-related systems. Our investigation is ongoing, and we may notify

additional individuals as our analysis proceeds. A copy of the sample breach letters for individuals is attached.

Sincerely,

Patrick Ray
General Counsel
The North Highland Company, LLC
Patrick.Ray@northhighland.com

NORTH HIGHLAND
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 23, 2022

i3623-L05-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L05
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to notify you that North Highland recently experienced a security incident that may involve your personal information. This incident affects personal information of current and former employees, as well as personal information that employees and former employees provided to us relating to their dependents and beneficiaries.

What Happened? On June 6, 2022, North Highland discovered that it had been the victim of a ransomware attack that impacted a number of on-premises servers. We initiated an investigation shortly after discovering it with the assistance of multiple outside security experts. On June 28, 2022, we confirmed that personal information of current and at least some former employees had been exfiltrated by the attackers. Our investigation has also confirmed that personal information of at least some beneficiaries and dependents of North Highland employees and former employees had been exfiltrated. While our investigation is ongoing, we currently believe that the attackers gained access to our servers on or around May 26, 2022.

What Information Was Involved? The compromised files may include the following personal data about current and former employees: names, social security numbers, identity numbers, tax numbers, addresses, bank account numbers and other payroll information, personal phone and email addresses, dates of birth, benefits information, background check and employment screening information, performance related records, health-related information you may have provided to us, such as in connection with leave requests or an accommodation, and other employment-related information.

The compromised files may also include information that North Highland employees and former employees provided to us relating to their dependents and beneficiaries, including dependent and beneficiary names, social security numbers, identity numbers, addresses, dates of birth, and other benefits-related information. Please note that dependents and beneficiaries whose data we received from employees and former employees are receiving their own notification letters, separate from the notification letters addressed to employees and former employees.

What Are We Doing? In response to these events, we engaged external cybersecurity experts to help with the investigation and remediation of the incident. We notified law enforcement of the attack; this notification has not been delayed due to a law enforcement investigation. We have also initiated a number of technical remediation efforts, including new password requirements for all employees. Further, we have arranged to provide certain identity protection services to impacted employees, former employees, dependents and beneficiaries through Experian. Below is a description provided by Experian of Experian's® IdentityWorks℠:

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **December 31, 2022.** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**:

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 397-0038 by December 31, 2022**. Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(888) 397-0038,** toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). 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 (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 this Identity Restoration support is available to you for 24 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. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Please note, the Experian activation code may only be used one time, and therefore cannot be shared by multiple people. Dependents and beneficiaries whose data we received from employees and former employees are receiving separate codes from the codes provided to employees and former employees.

What Can You Do? Please review the "Further Steps and Contact List" information on the reverse side of this letter which identifies additional steps to take to protect your information. If you have additional questions or concerns about this incident, please contact incidenthelp@northhighland.com.

Please know that we take the privacy and security of your personal information very seriously. We deeply regret any inconvenience this incident may cause you, and thank you for your understanding. **Please Note:** We will **NOT** send you any electronic communications regarding this incident that would involve a request to disclose any personal information.

Sincerely,

Patrick Ray (General Counsel)
Matt Klein (Managing Director & Chief Marketing Officer)
Paul Falor (Chief Information Officer)
incidenthelp@northhighland.com
1-888-730-9879

FURTHER STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION AND CONTACT LIST

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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact each one of the three national credit reporting agencies (contact information below).

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: A security freeze 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. Under federal law, you may not be charged to place or remove a credit freeze.

Police Report: If you file a police report, you have the right to obtain a copy of it.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, FTC (https://www.identitytheft.gov/) or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. You may want to contact your state Attorney General to obtain further information (see https://www.usa.gov/state-attorney-general). Below is the contact information for the Attorneys General for residents of New York, North Carolina, Rhode Island, Oregon, the District of Columbia, and Maryland.

Federal Trade Commission	**New York Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Office of the Attorney General The Capitol Albany, NY 12224-0341 https://ag.ny.gov/ 1-800-771-7755	9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400

Oregon Attorney General
100 SW Market Street
First Floor
Tilikum Room
Portland, OR 97201
https://www.doj.state.or.us/consumer-protection/
1-877-877-9392

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
oag@dc.gov
https://oag.dc.gov/

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://www.marylandattorneygeneral.gov/
Main number: 410-576-6300
Toll-free: 1-888-743-0023
Consumer Hotline: 410-528-8662

Contact Information for Credit Reporting Agencies:

	Equifax	Experian	TransUnion
To obtain a copy of your credit report	P.O. Box 740241 Atlanta, GA 30374 (866) 349-5191 www.equifax.com	P.O. Box 4500 Allen, TX 75013 (888) 397-3742 www.experian.com	P.O. Box 1000 Chester, PA 19016 (800) 888-4213 www.transunion.com
To obtain a security freeze	PO Box 105788 Atlanta, GA 30348 (800) 685-1111 www.equifax.com/personal/credit-report-services	PO Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 (888) 909-8872 www.transunion.com/credit-freeze
To place a fraud alert	P.O. Box 105069 Atlanta, GA 30348 (888) 766-0008 www.equifax.com/personal/credit-report-services	P.O. Box 2002 Allen, TX 75013 (888) 397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 (800) 680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert