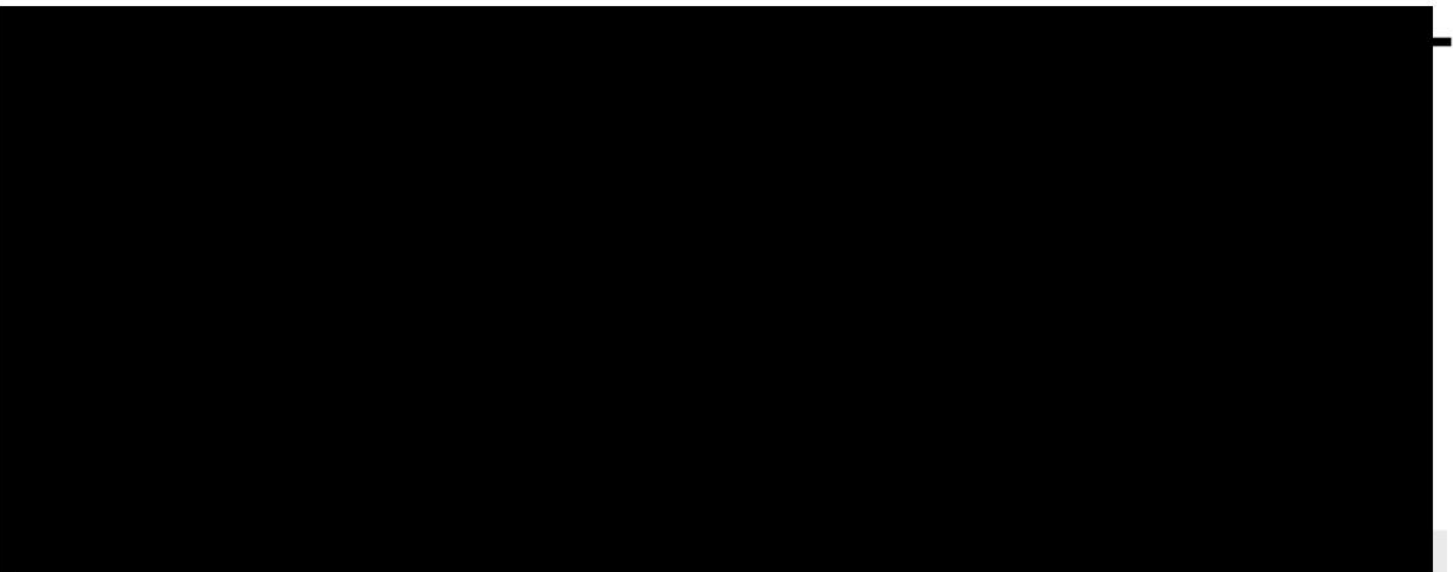




To Whom It May Concern:

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. The attack may have affected the following information relating to North Highland employees and former employees: 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 you may have provided to us, such as in connection with leave requests or an accommodation, and other employment-related information. We have since determined that personal information pertaining to at least 79 individuals from Maryland were or may have been impacted. Our investigation is ongoing, and we may notify additional individuals as our analysis proceeds. We are continuing to assess the extent of those affected and will make additional notifications in accordance with our assessment.

We intend to notify current employees on 7/8/22 and intend to notify former employees for whom we have readily available contact information in our HR system by 7/15/22. This population of former employees includes information on employees dating back to approximately 2014. A copy of the sample breach letters for individuals is attached. In addition to these two planned notices, we expect to make some additional notifications as our investigation proceeds. We are continuing to assess the extent of those affected, and will send additional notices in accordance with our findings.

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

Sincerely,

Patrick Ray
General Counsel
Patrick.Ray@northhighland.com

On Behalf of Patrick Ray,
Rodney Shanks | Davis Wright Tremaine LLP
Pronouns: he/him/his

Paralegal
920 Fifth Avenue, Suite 3300 | Seattle, WA 98104
Tel: (206) 757-8863 | Mobile: (206) 519-7541 | Fax: (206) 757-7700
Email: rodneyshanks@dwt.com | Website: www.dwt.com

Why am I sharing my pronouns? I simply want to show respect to the people who are regularly questioned about their gender and to help normalize the practice of sharing pronouns to promote inclusivity.

NORTH HIGHLAND

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

July 8, 2022

i0793-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL
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 experienced a security incident that involves your personal information.

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 files containing personal information of current and at least some former employees had been exfiltrated by the attackers. 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 of current and former employees: 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, health-related information you may have provided to us, such as in connection with leave requests or an accommodation, and other employment-related information.

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. Below is a description provided by Experian of Experian's® IdentityWorksSM:

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. 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**: October 31st, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **ABCDEFGHI**

3333 Piedmont Road NE | Suite 1000 | Atlanta, GA 30305 | 888.730.9879

North Highland® is a registered service mark of The North Highland Company

0000001



i0793-L01

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 (833) 420-2835 by October 31st, 2022 from Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Be prepared to provide engagement number **B055513** 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 (833) 420-2835 from Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (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.

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

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

New York Attorney General
Office of the Attorney
General
The Capitol
Albany, NY 12224-
0341
https://ag.ny.gov/
1-800-771-7755

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C.
20001
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

Rhode Island Attorney General
150 South Main
Street
Providence, RI
02903
http://www.riag.ri.gov
401-274-4400

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



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 initially determined that the personal information pertaining to 79 individuals from Maryland was or may have been impacted, and have since determined that the personal information of at least 116 individuals from Maryland was or may have been impacted.

We notified current employees on July 8, 2022. 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.

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

On behalf of Patrick Ray,
Rodney Shanks | Davis Wright Tremaine LLP
Pronouns: he/him/his
Paralegal
920 Fifth Avenue, Suite 3300 | Seattle, WA 98104
Tel: (206) 757-8863 | Mobile: (206) 519-7541 | Fax: (206) 757-7700
Email: rodneyshanks@dwt.com | Website: www.dwt.com

Why am I sharing my pronouns? I simply want to show respect to the people who are regularly questioned about their gender and to help normalize the practice of sharing pronouns to promote inclusivity.

NORTH HIGHLAND

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

July 8, 2022

i0793-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL
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 experienced a security incident that involves your personal information.

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 files containing personal information of current and at least some former employees had been exfiltrated by the attackers. 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 of current and former employees: 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, health-related information you may have provided to us, such as in connection with leave requests or an accommodation, and other employment-related information.

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. Below is a description provided by Experian of Experian's® IdentityWorksSM:

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. 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**: October 31st, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **ABCDEFGHI**

3333 Piedmont Road NE | Suite 1000 | Atlanta, GA 30305 | 888.730.9879

North Highland® is a registered service mark of The North Highland Company

0000001



i0793-L01

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 (833) 420-2835 by October 31st, 2022 from Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Be prepared to provide engagement number **B055513** 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 (833) 420-2835 from Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (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.

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

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

New York Attorney General
Office of the Attorney
General
The Capitol
Albany, NY 12224-
0341
https://ag.ny.gov/
1-800-771-7755

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C.
20001
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

Rhode Island Attorney General
150 South Main
Street
Providence, RI
02903
http://www.riag.ri.gov
401-274-4400

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

NORTH HIGHLAND

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

July 27, 2022



i1422-L05-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L05 FORMER EMP & DEP US

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® IdentityWorksSM:

3333 Piedmont Road NE | Suite 1000 | Atlanta, GA 30305 | 888.730.9879

North Highland® is a registered service mark of The North Highland Company

0000001



i1422-L05

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. 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: October 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: ABCDEFGHI**

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 **(833) 420-2835 by October 31, 2022**. Be prepared to provide engagement number **B055649** 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 ExtendCARETM:** 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 **(833) 420-2835**, 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

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

New York Attorney General

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
<https://ag.ny.gov/>
1-800-771-7755

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>
401-274-4400

0000001



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

NORTH HIGHLAND

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

July 27, 2022

i1422-L12-0000008 T00001 P001 *****SCH 5-DIGIT 12345

PARENT OR GUARDIAN OF

SAMPLE A SAMPLE - L12 MINOR DEPENDENT US

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



NOTICE OF DATA BREACH

Dear Parent or Gaurdian of Sample A. Sample:

We are writing to notify you that North Highland recently experienced a security incident that may involve your minor's 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 has been exfiltrated. Your minor's information may have been among the data acquired by the attackers. 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 personal data that North Highland employees provided to us relating to their dependents and beneficiaries, including dependent or beneficiary social security numbers, addresses, and dates of birth. 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. We have also initiated a number of technical remediation efforts, including new password requirements for all employees. Below is a description provided by Experian of Experian's® IdentityWorksSM



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

- Ensure that you **enroll by: October 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/minorplus
- Provide your **activation code: ABCDEFGHI**
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 420-2835** by **October 31, 2022**. Be prepared to provide engagement number **B058222** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding the 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 for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** Receive the same high-level of Identity Restoration support even after the 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 minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent **(833) 420-2835**, 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 your minor 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.

* 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 and your minor's 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 and your minor's personal information very seriously. We deeply regret any inconvenience this incident may cause, 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

0000008



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

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

New York Attorney General

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
<https://ag.ny.gov/>
1-800-771-7755

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>
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

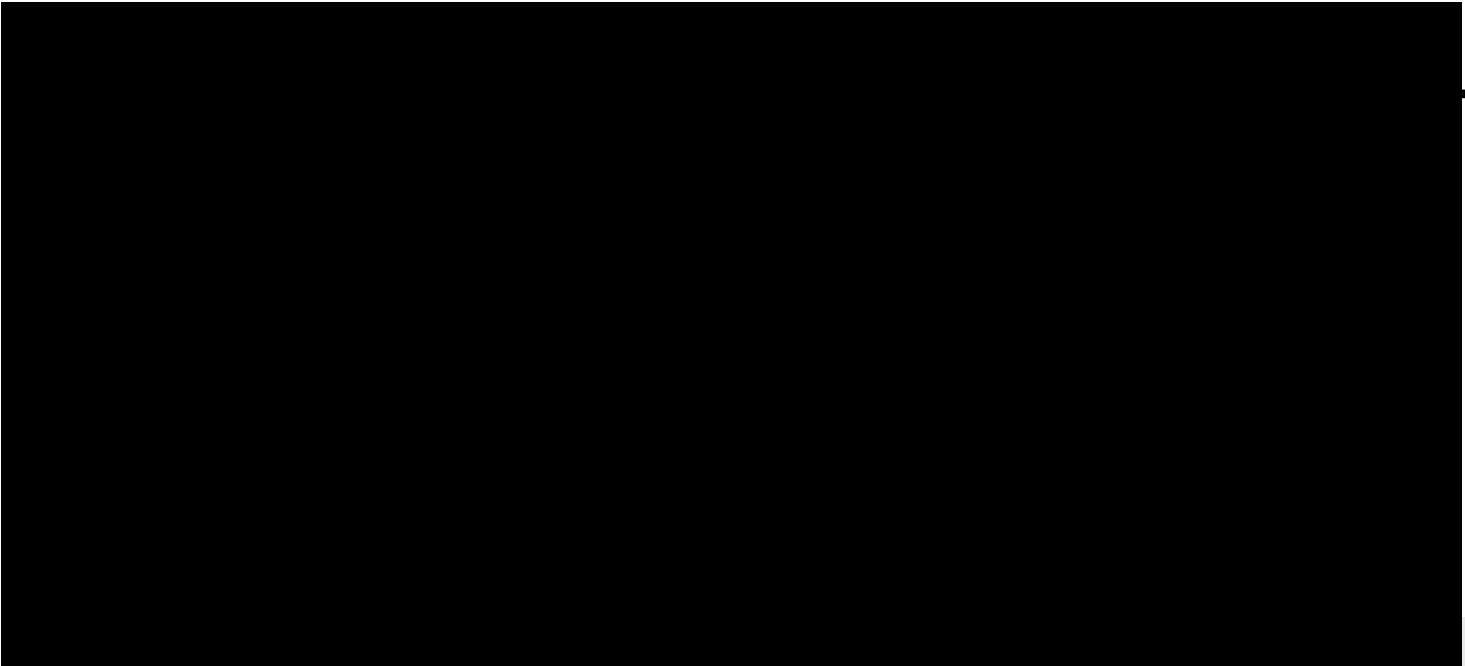
400 6th Street NW
Washington, D.C. 20001
oag@dc.gov
<https://oag.dc.gov/>

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



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. Our previous notification dated July 7th, 2022 is attached and our notification dated July 27th is in the email chain below. 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.

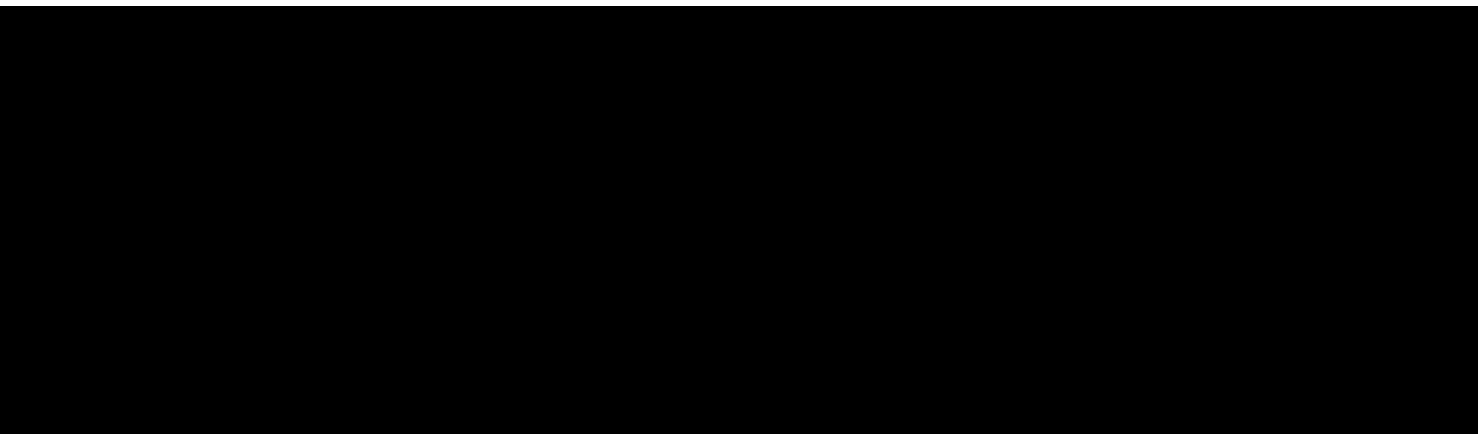
We have now completed our investigation. We found an additional 53 residents of Maryland since our last notice, resulting in a total number of 169 individuals affected in Maryland for this incident. We have notified the additional 53 residents of Maryland on August 10, 2022 and September 23, 2022. The sample breach letter sent to all additional residents is substantively the same as the sample notices we previously provided. A copy of the sample breach letter sent to additional residents is attached.

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

Sincerely,

Patrick Ray
Patrick.Ray@northhighland.com

On Behalf of Patrick Ray,
Rodney Shanks | Davis Wright Tremaine LLP
Paralegal



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® IdentityWorksSM:

3333 Piedmont Road NE | Suite 1000 | Atlanta, GA 30305

North Highland® is a registered service mark of The North Highland Company

0000001



i3623-L05

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. 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: ABCDEFGHI**

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 **B061838** 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 ExtendCARETM:** 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

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

New York Attorney General

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
<https://ag.ny.gov/>
1-800-771-7755

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>
401-274-4400

0000001



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