

KING & SPALDING

King & Spalding LLP
1700 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
www.kslaw.com

Robert Hudock, Partner
Direct Dial: +1 202-626-5521
rhudock@kslaw.com

Adam Solander, Partner
Direct Dial: +1 202-626-5542
asolander@kslaw.com

November 25, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Via electronic mail

Re: Notice of Security Incident Affecting Northern Safety Company, Inc.

To Whom It May Concern:

We write on behalf of Northern Safety Company, Inc. (“NSC”) regarding a security incident.

On June 7, NSC detected some unusual activity directed toward its network. NSC subsequently experienced a criminal ransom-related event where an unauthorized party, later identified as ransomware group Black Basta, claimed to have accessed parts of NSC’s network and exfiltrated some company data. NSC immediately notified the Federal Bureau of Investigation (“FBI”) of the activity and engaged third-party cybersecurity experts to assist with analysis and containment measures.

The FBI took a particular interest in this incident due to the unique characteristics of this threat actor group and incident. Black Basta is known for highly targeted and sophisticated attacks. NSC actively cooperated with the FBI over the course of several months to assist with the Bureau’s investigation. The investigation was complicated due to the threat actor group’s inconsistent and erratic activity.

While the FBI investigation proceeded, NSC, through the assistance of the FBI and its cybersecurity experts, identified the root cause of the incident and restored NSC systems to normal business operations. NSC undertook an extensive analysis of the impacted data to determine if the data contained any personal information and (if so) which individuals and data may have been affected by the incident. The data analysis was a highly technical, energy intensive process due to

the quantity of impacted data and its unstructured nature. Approximately 750 gigabytes of data were impacted by the incident, the vast majority of which was unstructured text in the form of comma-delimited files, such as sales information for commercial safety equipment (like safety cones and safety vests) and was not personal information subject to the state's data breach notification law.

On or about October 25th, NSC determined that the personal information of approximately 3 Maryland residents may have been accessed, all of whom appear to be existing or former employees or workforce members of the company. Based on its investigation, NSC identified that personal information that may have been accessed may include one or more data elements consisting of names, addresses, email addresses, telephone numbers, dates of birth, Social Security numbers, or employee benefits related information. Therefore, NSC will be sending notices, a copy of which is attached, to impacted residents via USPS First Class Mail on or about the date of this letter.

By virtue of this notice, NSC does not waive any rights and reserves all rights under applicable law. Please do not hesitate to contact us if you have any questions regarding this letter.

Sincerely,

/s/ Robert Hudock
Robert Hudock

/s/ Adam Solander
Adam Solander

Encl.: Individual Notice Letter Template

Return Mail Processing
PO Box 999
Suwanee, GA 30024

11 1 1873 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



November 25, 2024

Re: NOTICE OF DATA BREACH

Dear Sample A. Sample:

Northern Safety Co., Inc. writes to inform you of a recent security incident that may involve your information. Although we are unaware of any actual misuse of your information, we want to let you know about the incident, steps we are taking in response, and steps you may take to help protect your personal information against identity theft or other misuse, should you feel it is appropriate to do so.

What Happened?

On June 7, we detected some unusual activity directed toward our network. We subsequently experienced a criminal ransom-related event where an unauthorized party claimed to have accessed parts of our network and exfiltrated some company data. We immediately notified law enforcement of the activity and engaged third-party cybersecurity experts to assist with analysis and containment measures.

We actively cooperated with law enforcement over the course of several months to assist with their investigation, which was complicated by the unauthorized party's inconsistent and erratic activity. We undertook an extensive analysis of the impacted data to determine if the data contained any personal information and (if so) which individuals and data may have been affected by the incident. The overwhelming majority of the data was not personal information and related to old business records such as historical sales information for commercial safety equipment (like safety cones and safety vests).

On October 25, we completed our initial analysis and determined that the personal information of some of our current and past employees (and/or their beneficiaries) was among the potentially impacted data, including your personal information. We are unaware of any actual misuse of this information. Out of an abundance of caution, we are providing you with services and tools to help you protect yourself. Those services are described below.

What Information Was Involved?

Based on our investigation to date, the data accessed includes some or more of the following

data of yours: name, address, email address, telephone number, date of birth, Social Security Number, and employer information related to benefits enrollment.

What Are We Doing?

Immediately upon learning of the security incident, we began reviewing all its aspects and took steps to protect the systems involved. We worked with outside experts to assess the incident and safely restore our systems, including reviewing and enhancing our system security and administrative and technical safeguards.

As an additional measure of protection, we are providing you with complimentary credit monitoring services through Experian.

What Can You Do?

As always, we recommend that you remain vigilant and review your account statements and free credit reports regularly and report any concerning transactions to your financial provider.

We encourage you to contact Experian to enroll in credit monitoring and related services described below under “Additional Resources.” You can also review the “Additional Resources” section of this letter for additional ways to help protect yourself. They include recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file.

For More Information

We regret any inconvenience or concern this incident may have caused. If you have questions about the incident, please call 833-918-1108 toll-free Monday through Friday from 8 am – 8 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B133650.

Sincerely,

Tammy Marchese
Northern Safety Human Resources Department

ADDITIONAL RESOURCES

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, including exercising your right to file a police report. You may also contact your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you 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 access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>.

Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

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>.

Credit Report Monitoring & Identity Theft Protection Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twenty-four (24) months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** February 28, 2025 (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

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-1108 by February 28, 2025 (5:59 UTC). Be prepared to provide engagement number B133650 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 specialists 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.

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

- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. For more information, please visit [IdentityTheft.gov](https://www.identitytheft.gov) or call 1-877-ID-THEFT (877-438-4338).

Security Freeze

In some U.S. states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.

State Information on Preventing and Responding to Identity Theft

You may want to review any materials your state provides regarding identity theft and credit monitoring that may provide additional information and resources to protect yourself against any risks. Below is a list of state resources that may be helpful to review for additional information.

District of Columbia residents: May obtain information on how to minimize identity theft risks provided by the Office of the Attorney General for the District of Columbia at <https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft>, or by calling (202) 727-3400 or writing to the Office of the Attorney General at 400 6th Street NW, Washington, D.C. 20001.

Florida residents: May obtain information on how to minimize identity theft risks provided by the Florida Attorney General at <https://www.myfloridalegal.com/identity-theft/identity-theft-victim-kit>.

Louisiana residents: May obtain information from the Louisiana Department of Revenue at <https://revenue.louisiana.gov/TaxFraud/IdentityTheft>. The Louisiana Department of Revenue also provides an "Identity Theft Checklist" at <https://revenue.louisiana.gov/FraudForms/IdentityTheftChecklist.pdf>.

** 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.

Maryland residents: May wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or writing to the Office of the Attorney General at 200 St. Paul Place, Baltimore, MD 21202, or calling 1-888-743-0023 (toll free) or 410-576-6491.

New Hampshire residents: May obtain information about steps for victims of identity theft from the Consumer Protection and Antitrust Bureau of New Hampshire's Department of Justice, Office of the Attorney general at <https://www.doj.nh.gov/consumer/identity-theft/index.htm>.

New Jersey residents: May obtain information about preventing identity theft from the Division of State Police in the Department of Law and Public Safety at <https://www.nj.gov/njsp/tech/identity.html>.

New York residents: May obtain information about preventing and responding to identity theft from the New York State Department of State Division of Consumer Protection at <https://dos.ny.gov/protecting-yourself-identity-theft>, which also links to a comprehensive guide <https://dos.ny.gov/system/files/documents/2018/06/idtheftbrochure.pdf>.

North Carolina residents: May obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

Texas residents: May obtain information on helping prevent identity theft provided by the Texas Attorney General at <https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/help-prevent-identity-theft>.

Virginia residents: May obtain information by viewing the comprehensive guide for identity theft victims provided by the Virginia Attorney General at [https://www.oag.state.va.us/consumer-protection/files/ID Theft Booklet 2016 web.pdf](https://www.oag.state.va.us/consumer-protection/files/ID%20Theft%20Booklet%202016%20web.pdf).

Washington residents: May obtain information by reviewing the "Identity Theft/Privacy" section of the Washington Attorney General's website at <https://www.atg.wa.gov/guardit.aspx>.

Wisconsin residents: May obtain information by reviewing Wisconsin's Department of Agriculture, Trade and Consumer Protection's ID Theft/Privacy Protection Fact Sheets at <https://datcp.wi.gov/Pages/Publications/IDTheftPrivacyProtectionFactSheets.aspx#:~:text=Credit%20Report%20Security%20Freeze,help%20protect%20from%20identity%20theft>.