

Kelley M. Donnelly
248.727.1609
kdonnelly@taftlaw.com

July 6, 2023

Office of the Maryland Attorney General
Saint Paul Plaza
200 St. Paul Place
Baltimore, MD 21202

IDTheft@oag.state.md.us.

Dear Attorney General Brown:

We represent Northern Engraving Corp (the “Company”) in connection with a recent data security incident. We are writing to inform your offices of this incident and provide the requisite information pursuant to Maryland Commercial Code §14-3504(h).

(i) The number of affected individuals residing in the State:

There is only one affected individual residing within the state of Maryland.

(ii) A description of the breach of the security of a system, including when and how it occurred:

The breach of the Company's security system occurred on May 12, 2023 as a result of a ransomware attack. The breach was discovered that same day and steps were immediately taken to secure the Company's network. The categories of information possible access and/or obtained may include employees': (a) name; (b) address; (c) social security number; (d) telephone number; (e) date of birth; and (f) financial account information. The Company has no evidence that any personal information was compromised or misused in any manner, however, the Company is proactively taking precautionary measures.

(iii) Any steps the business has taken or plans to take relating to the breach of the security of a system:

Within one hour of becoming aware of the incident, Northern Engraving disconnected all external network links to isolate its datacenter. Northern Engraving's IT

Director, within two hours of the incident occurring coordinated with his IT team to determine what happened and to coordinate external IT service providers to assist with Northern Engraving's incident response. Heartland Business Systems ("Heartland") arrived on site to assist with scanning all workstations and data points to determine the attack vector. Heartland assisted Northern Engraving's IT team onsite with cleaning and/or sanitizing all workstations and servers. Computer Forensic Services were also retained to analyze infected drives. All accounts were disabled.

The following additional data security safeguards were implemented: change password requirements to make them more stringent; removed infected server stack from environment; restored servers from an air gap backup that was known to be clean; purchased all new datacenter servers to ensure none were infected with any advanced persistent threats or any other threats; passwords for all firewalls and network devices were changed; added restrictions to access datacenters, restricting access through access lists and employing a zero trust model; updated antivirus software to a more robust service on all services, which are monitored 24/7 by Sophos MDR; updated and changed network segmentation to isolate Northern Engraving's data center key assets; implement stricter MFA security requirements and rules, including the implementation of geography restrictions and code entry; shutdown external access to the Citrix environment; integrated Azure MFA with Northern Engravings VPN; and removed all devices with OS older than Windows 10 from the network (only key devices with Windows 7 were allowed back on the network once it was verified they were clean and had Sophos legacy support installed). Northern Engraving is and will continue to add additional data security safeguards to its information infrastructure, including additional activity monitoring and automatic shutdown processes that identify suspicious activity.

At this time, the Company does not believe and has no evidence to believe otherwise that sensitive information of any individual was accessed or compromised. Nevertheless, as detailed in the Notification Letter, the Company is providing all affected individuals with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge for 24 months from the date of enrollment.

In addition, the Company established a toll free call center through Cyber Scout, to answer any questions about the incident and address related concerns. The call center is available at 1-833-770-0794 from 8:00 AM to 8:00 PM EST, Monday through Friday (excluding holidays).

(iv) The form of notice that will be sent to affected individuals and a sample notice:

The form of notice is enclosed with this correspondence.

Office of the Maryland Attorney General
July 6, 2023
Page 3

The Company remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact us.

Sincerely,

Taft Stettinius & Hollister LLP

Kelley M. Donnelly

KMD
Enclosure: Sample Notification Letter
CC: Jon Sriro (jsriro@taftlaw.com)

Northern Engraving Corp.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07561 1-1



July 5, 2023

Re: Personal Information of [REDACTED]

Dear [REDACTED]

Please read this letter in its entirety.

I am writing to inform you of a cyber-security incident affecting Northern Engraving Corp. ("Northern Engraving"). As a current or former employee of Northern Engraving, certain personal information retained by Northern Engraving related to your employment may have been compromised during this incident.

What happened?

On May 12, 2023, Northern Engraving discovered that our server was the victim of a malware attack. Once we discovered the cyber-attack, we took immediate steps to mitigate any potential impact. We also began an investigation into this incident, which is still ongoing.

What information was taken?

During the ransomware attack, the personal information you provided to NBHX USA during your employment may have been compromised. The personal information you provided to Northern Engraving during your employment may have been included in those records. The categories of information possibly accessed and/or obtained may include employees': (a) name; (b) address; (c) social security number; (d) telephone number; (e) date of birth; and (f) financial account information. **While we have no evidence that any of your personal information was compromised or misused in any manner, we are proactively taking precautionary measures to ensure your financial security and alleviate concerns you may have.**

What we are doing.

Immediately upon discovering the breach, Northern Engraving took swift action and engaged a third-party forensic team to determine what data, if any, was accessed. The company also retained separate technical support to address any deficiencies in its data security. These investigations and support efforts are ongoing.

How do I enroll for the free services?

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/northengcorp> and follow the instructions provided. When prompted please provide the following unique code to receive services: **JPYSD8LRXF**. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What you can do.

Cyberscout has been retained to answer your questions or address problems you may encounter. This could include helping you obtain a credit report and placing fraud alerts. However, if you choose not to use these services, we are strongly urging all employees to place their own fraud alert and obtain and monitor a credit report.

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report by visiting: www.annualcreditreport.com or by calling toll-free at 1-877-322-8228. (Hearing-impaired consumers can access their TDD service at 1-877-730-4204).
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- **Promptly report any suspicious activity to Cyberscout.**

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC) by visiting www.ftc.gov/idtheft. The FTC also has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261.

What if I want to speak with Northern Engraving regarding this incident?

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line 1-833-770-0794 and supply the fraud specialist with your unique code listed above.

Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding the protection of your personal information. You can also review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud."

We take the privacy and security of your protected personal information seriously and have worked diligently to provide you with support and assistance. We sincerely regret any inconvenience or concern this incident may cause you and strongly encourage the utilization of Cyberscout's services.

Sincerely,
Northern Engraving

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

File Your Tax Return. If you have not already done so, we encourage you to file your 2022 tax return as soon as possible. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look at the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit <http://www.taxadmin.org/state-tax-agencies>.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. You should not be charged to place or lift a credit freeze or security freeze on your credit file. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Additional Information

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation.