CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

ERNEST KOSCHINEG
ekoschineg@c-wlaw.com

JORDAN MORGAN
jmorgan@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

February 22, 2021

Via Mail
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Security Incident Notification

To Whom It May Concern:

I serve as counsel for Maine Drilling and Blasting ("Maine"), and provide this notification to you of a recent data security incident suffered by Maine. On or about January 29, 2021, Maine Drilling and Blasting became aware of a ransomware threat that had attacked their network. Upon discovery, Maine immediately secured their network and engaged a third-party forensic company to investigate. Maine dedicated all of their IT and engineering resources to resolve the problem and restore our network. Following the forensic experts' progress in their thorough investigation, it was ultimately determined that our computer network was accessed by an unknown individual shortly before the ransom attack took place. Upon confirmation of this unauthorized access, Maine's third-party forensic experts immediately investigated whether the affected databases contained individuals' sensitive information. Through their investigation, Maine determined that the incident may have the limited personal information of their employees.

On February 10, 2021, Maine discovered that Ninety (90) New Hampshire residents may have been affected by this incident. As our investigation is ongoing, we will provide supplemental notification should we determine additional New Hampshire residents are potentially affected.

Maine promptly notified the affected individuals via First Class Mail on February 20, 2021 and is offering all affected individuals complimentary credit monitoring for two (2) years. A copy of the draft notification letter is attached, which outlines the incident and provides affected individuals with additional resources to protect their identity and monitor the credit history and personal accounts. As the letter indicates, Maine will be offering credit monitoring services at Maine's expense through Norton LifeLock. Maine is taking proactive steps to ensure that all state and federal notification obligations are complied with due to this incident.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: Jordan L. Morgan
Jordan L. Morgan, Esq.

Maine Drilling
& Blasting
600 Satellite Blvd.
Suwanee, GA 30024

1 1 227 **********SNGLP
John Doe
123 Anystreet Dr
Anytown, NY 12345

February 22, 2021

RE: NOTICE OF DATA BREACH
Important Security Notification. Please read this entire letter.

Dear John Doe:

I am writing to inform you of a data security incident experienced by Maine Drilling and Blasting ("Maine") that may have involved your personal information described below.

Maine takes the privacy and security of all information very seriously. While we have no evidence to suggest that any of the impacted information was viewed or misused during this incident, it is crucial that we be as supportive and transparent as possible. That is why I am writing to inform you of this incident, and to offer information about steps that can be taken to help protect your information.

I sincerely apologize for any concern that this incident may cause you. Let me reassure you that Maine Drilling and Blasting is fully committed to supporting you.

What Happened:

On or about January 29, 2021, Maine Drilling and Blasting became aware of a ransomware threat that had attacked our network. Upon discovery, we immediately secured our network and engaged a third-party forensic company to investigate. We dedicated all of our IT and engineering resources to resolve the problem and restore our network. Following the forensic experts' progress in their thorough investigation, it was ultimately determined that our computer network was accessed by an unknown individual shortly before the ransom attack took place. Upon confirmation of this unauthorized access, Maine's third-party forensic experts immediately investigated whether the affected databases contained individuals' sensitive information, which is still ongoing.

To date, there is no indication that any of your information was actually viewed, misused, or disclosed by any third-party during this compromise. We are providing this notification to you out of an abundance of caution and so that you may diligently monitor your personal information and resources. We take great care in the protection of your information and regret that this incident has occurred.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that any personally identifiable information has been misused in connection to this incident. The personal information that could have been viewed by the unauthorized individual(s) may have included your first name and last name, in combinations with your:

- Social security number,
- Drivers license number or other identification numbers,
- Date of birth,
- Tax identification number,
- Bank or other financial account information,
- Credit or debit card informaton, and/or your
- Protected health information such as:
    - Treatment and diagnosis information, prescription information, provider name, medical record number, Medicare or Medicaid number, and health insurance information.

Importantly, the information potentially impacted as it relates to you may be limited to only one of the above-listed types of information.

What We Are Doing:

Maine has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Unfortunately, network intrusions have become more common and this incident experienced by Maine is similar to experiences by other companies across a range of industries and practice areas. Upon learning of this incident, we immediately secured the affected accounts, reset passwords, and took steps to enhance the security of all information to help prevent similar incidents from occurring in the future. Furthermore, we retained a third-party forensic firm to conduct a thorough investigation of the incident.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, please report an suspicious incidents to local law enforcement and/or your State Attorney General. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact me at 207-203-1605

Maine Drilling and Blasting has no relationship more important or more meaningful than the one we share with you. I want to personally express my deepest regret for any worry or inconvenience that this incident may cause you.

Sincerely,

Dan Werner
President and CEO

Maine Drilling & Blasting has retained **NortonLifeLock** to provide twenty-four (24) months of complimentary **LifeLock Defender™ Preferred** identity theft protection.

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to **www.LifeLock.com**. Click on the yellow **"START MEMBERSHIP"** button (*do not attempt registration from a link presented by a search engine).*
2. You will be taken to another page where, below the FOUR protection plan boxes, you may enter the **Promo Code:** [redacted] and click the **"APPLY"** button.
3. On the next screen, enter your **Member ID:** [redacted] and click the **"APPLY"** button.
4. Your complimentary offer is presented. Click the red **"START YOUR MEMBERSHIP"** button.
5. Once enrollment is completed, you will receive a confirmation email (*be sure to follow ALL directions in this email*).

Alternatively, to activate your membership over the phone, please call: (866) 913-7428.

You will have until June 18th, 2021 to enroll in this service. Please activate now as late enrollments will not be accepted.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Defender™ Preferred** membership includes:

- ✓ Primary Identity Alert System†
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring**
- ✓ Norton™ Security Deluxe[2] (90 Day Free Subscription)
- ✓ Stolen Funds Reimbursement up to $25,000†††
- ✓ Personal Expense Compensation up to $25,000†††
- ✓ Coverage for Lawyers and Experts up to $1 million†††
- ✓ U.S-based Identity Restoration Team
- ✓ Annual Three-Bureau Credit Reports & Credit Scores[1]**
  The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.
- ✓ Three-Bureau Credit Monitoring[1]**
- ✓ USPS Address Change Verification Notifications
- ✓ Fictitious Identity Monitoring
- ✓ Credit, Checking and Savings Account Activity Alerts†**

[1]If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.

No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.

[2] Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.

**These features are not enabled upon enrollment. Member must take action to get their protection.

††† Reimbursement and Expense Compensation, each with limits of up to $25,000 for Defender Preferred. And up to $1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion	**Experian**	**Equifax**
Fraud Victim Assistance Dept.	National Consumer Assistance	Consumer Fraud Division
P.O. Box 2000	P.O. Box 9554	P.O. Box 740256
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30374
1-800-680-7289	1-888-397-3742	1-800-525-6285
www.transunion.com	www.experian.com	www.equifax.com

➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. In order to request a security freeze,you will need to provide some or all of the following informationto the credit reporting agency, depending on whether you do so online, by phone, or by mail: 1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security Number; 3. Date of birth; 4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address,suchas a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2;8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

➢ USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements.
Be proactive and create alerts on credit cards and bank accounts to notify you of activity.

If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE**

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

- **RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)**

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit "prescreened" offers of credit an insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.

- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.

- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

- **For New York residents,** you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotectionl; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

- **For North Carolina residents,** the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

- **For Rhode Island Residents,** the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov or 401-274-4400.