

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700

Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

JORDAN MORGAN
jmorgan@c-wlaw.com

LEI WANG
lwang@c-wlaw.com

April 14, 2024

Via E-Mail (IDTheft@oag.state.md.us)

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

RE: Security Breach Notification

To Whom It May Concern:

We serve as counsel for Hill Mechanical Corp. ("Hill"), located at 11045 Gage Avenue, Franklin Park, IL 60131, and provide this notification to you of a recent data security incident suffered by Hill. By providing this notice, Hill does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around November 16, 2023, Hill became aware of potential unauthorized access to an employee email account. Upon discovery, Hill immediately performed a password reset for the affected account and swiftly engaged a third-party team of forensic investigators in order to determine the full nature and scope of the incident. Following a thorough investigation, Hill confirmed that a limited amount of personal information may have been accessed in connection with this incident.

On March 25, 2024, Hill discovered one (1) Maryland resident may have been affected by this incident. The type of information that could have been accessed included name and Social Security number. As our investigation is ongoing, we will provide supplemental notification should we determine additional residents of Maryland are potentially affected.

Hill will provide written notification to the potentially impacted Maryland resident via First Class Mail on April 15, 2024, pursuant to Maryland law. The notification letter includes details of the incident and an offer of complimentary credit monitoring and identity protection services for 12 months and access to a dedicated call center. A copy of the notification letter is attached hereto as **Exhibit A**.

Please contact me should you have any questions.

Very truly yours,

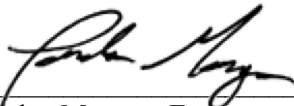

Jordan Morgan, Esq.

Exhibit A

Hill Mechanical Corp.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB08727 19-1



[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

April 15, 2024

RE: Important Security Notification. Please read this entire letter.

Dear [REDACTED],

Hill Mechanical Corp. ("Hill") writes to notify you of a recent incident that may have impacted some of your personal information described below.

We take the privacy of information in our care seriously, and while we have no evidence to suggest that any information has been misused, in an abundance of caution, we are providing you information about the incident, our response, and steps you can take to protect your information.

What Happened:

On or around November 16, 2023, Hill became aware of potential unauthorized access to an employee email account. Upon discovery, we immediately performed password resets for the affected account and swiftly engaged a third-party team of forensic investigators in order to determine the full nature and scope of the incident. On March 25, 2024, following a thorough investigation, we discovered that a limited amount of personal information may have been accessed by an unauthorized third party in connection with this incident.

At this time, there is no indication that any information has been misused. However, we are providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel it is necessary to do so.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that any information has been misused. The information that could have been accessed by the unauthorized individual(s) may have included your first and last name, in combination with your Social Security number and driver license number.

What We Are Doing:

Hill has taken steps to address the incident and is committed to protecting personal information in its care. Upon learning of this incident, we immediately took steps to secure our systems, and to enhance the security of our network to prevent similar incidents from occurring in the future. As a additional safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for twelve (12) months provided by Cyberscout, a TransUnion company. Due to privacy laws, we cannot register you directly. Additional information regarding how to enroll in the complimentary credit monitoring service is enclosed.

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, 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 any of your accounts, please promptly change your password and take additional steps to protect your account, and notify your financial institution or company if applicable. Additionally, please report any 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 us at 1-833-543-2828, between the hours of 8:00 am and 8:00 pm Eastern time, excluding holidays, or write us at 11045 Gage Avenue, Franklin Park, IL 60131.

We take the security of information entrusted to our care very seriously. While it is regrettable this incident occurred, please be assured we are taking appropriate actions to rectify the situation and prevent such incidents in the future.

Sincerely,

James S. Billard
Vice President, Corp. Risk Management
Hill Mechanical Corp.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for twelve (12) 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, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://www.mytrueidentity.com> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. 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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms 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, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289	Experian 1-888-397-3742	Equifax 1-888-298-0045
-------------------------------------	-----------------------------------	----------------------------------

www.transunion.com	www.experian.com	www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, 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 employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are zero (0) residents of Rhode Island impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.