November 12, 2023

Hill International

Maryland Office of the Attorney General
Director of Consumer Affairs & Business Regulation
idtheft@oag.state.md.us

Dear Attorney General Brown:

Pursuant to Md. Code Com. §14-3501 et seq., we are writing to notify you of a breach of security involving **92** Maryland state residents.
`

1. **Brief Description**
   By way of background, Hill International, Inc (“Hill”) is a construction management and project management company in Philadelphia, PA. Hill operates exclusively on a business-to-business basis. The majority of personal data Hill processes is employee or contractor information.

   Hill discovered suspicious network activity resulting in a partial systems outage on June 10, 2023. Hill immediately launched its incident response procedure, engaged external experts to identify the cause of the incident; and notified the FBI.

   Hill identified that the incident was a ransomware attack deployed by the Threat Actor (TA), PLAY. Over the three days following initial discovery, Hill took steps to contain, remediate, and restore systems securely as quickly as possible. Containment and remediation were accomplished within three days. Hill was able to confirm that key HR systems containing employee or worker personal data were not impacted.

   Hill, with the assistance of external third-party experts and breach legal counsel conducted a thorough investigation into the incident determining the breach period began on March 23, 2023. Hill also engaged an expert data analytics firm to perform a detailed data mining exercise. It is at this stage following the output of the data mining exercise that Hill has become aware of the involvement of some personal data relating to **92** individuals that may be Maryland residents. It is on that basis that Hill is notifying the Maryland Attorney General’s office and potentially affected individuals.

2. **Notice to Individuals.**
   Notice of the security incident was sent to individuals on November 4, 2023. Hill is offering Kroll credit and identity monitoring services for at least one year to all potentially affected Marylanders.

   It is important to note, with any such event, it takes time to gather the relevant information, identify the scope of the incident, hold the necessary internal discussions, and make the appropriate decisions. This is particularly applicable in this case, where Hill was dealing with a complex and robust data set of primarily imaged (e.g. .pdf) and non-structured data.

3. Sensitive Personal Information

The data involved in the event may have included: full name; social security number; passport information, and state identification numbers.

4. Measure to Address the Security Incident

Hill made focused updates to its security program before, during, and after a critical review of the Incident to further enhance its security posture around an ever-changing threat landscape, which included:

Technical updates to the security infrastructure spanned:

- Deployment of early detection and response agents on all endpoints (laptops and servers);
- Engaging a new Managed Detection and Response (MDR) vendor;
- Increasing authentication thresholds to log into the Virtual Privacy Network (VPN);
- Instituting a global technical policy blocking USB ports without prior approval of the Director, Global Technical Services;

Hill also made several administrative and procedural enhancements to its security program, including:

- Stale laptops that have not connected to the Hill domain within 90 days are frozen until unlocked by IT;
- Security removed the ability of admin accounts to access the VPN and all VPN traffic is logged;
- A global password reset was executed for all users; and
- Local Admin Accounts were reset and all end users who may have Local Admin accounts were assessed for need and role by IT.

Hill also engaged a provider to monitor the dark and deep web for any indication that exfiltrated data was published or made available for sale or trade subsequent to the ransom. Monitoring was for an initial period of approximately two months directly after the incident and again, in an abundance of caution, throughout the month of October 2023. Monitoring provided no indication of improper use of data or direct risk to individuals.

5. Hill Security and Privacy Prior to the Incident

Prior to the incident, Hill had a variety of preventative measures in place, including but not limited to administrative, technical, and physical controls consistent with ISO27001 standards, Generally Accepted Privacy Principles (GAPP), and Standard Contractual Clauses for third-party vendors. These measures were regularly tested both internally and by third-party experts. Security and privacy policies undergo an annual review. Employees receive annual training on security and privacy as well as receiving awareness campaigns.

In addition to the above measures, since the Incident, Hill has been working to further reinforce its systems and has taken steps as described in section **4** above.

Should you require additional information, I can be reached at aileenschwartz@hillintl.com, privacyofficer@hillintl.com or by phone at (215) 309-7700.

Respectfully Submitted,

Aileen Schwartz
Senior Vice President, General Counsel Americas & Chief Privacy Officer Hill International, Inc.

Attachment (1)

HILL International

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Hill International, Inc. (Hill) is writing to notify you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On June 10, 2023, Hill discovered suspicious activity on its network and immediately launched our incident response which included engaging external experts to investigate the incident. The investigation determined that an unauthorized actor accessed the Hill network and removed certain files from it between March 23, 2023, and June 10, 2023. As a result, Hill undertook a comprehensive process to identify what information was potentially contained within the relevant files and to whom that information belonged. That review process was completed in mid-October 2023. We are now notifying individuals whose information was potentially impacted by the incident.

What information was involved?

Information that could have been subject to unauthorized access includes: Full Name; Date of Birth; Passport Number; Social Security Number; and Driver's License and State ID information.

Although Hill considers this to be extremely unlikely, due to the data categories involved, it is possible that the information could be used for identity theft or fraud. We and our experts continue to monitor for disclosures of data related to this event. We are not aware of any risk to you directly as a result of this incident.

What we are doing.

Upon discovery of this incident, we launched an in-depth investigation with the assistance of third-party forensic specialists to determine the nature and scope of this incident. As part of our ongoing commitment to the privacy of information in our care, we are reviewing and updating our existing policies and procedures and implementing additional safeguards to further secure the information in our systems as appropriate. We notified law enforcement and are notifying regulatory authorities as required by law. We are also notifying potentially affected individuals, including you, so that you may take further steps to help protect your personal information, should you feel it is appropriate to do so. As an added precaution, to help relieve concerns and restore confidence following this incident we arranged to have **Kroll** provide identity monitoring services at no cost to you for one year.

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your Identity Monitoring Services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

> Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your Identity Monitoring Services.
>
> *You have until **<<b2b_text_6 (activation date)>>** to activate your Identity Monitoring Services.*
>
> Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring Services, you can visit info.krollmonitoring.com.[1]

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

We understand you may have additional questions not addressed by this letter. If you have questions, please reach out to eventinfo@hillintl.com which will be routed to the Hill International Chief Privacy Officer. You may also call our dedicated assistance line at **<<TFN>>**, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Aileen R. Schwartz
Senior Vice President, General Counsel Americas & Chief Privacy Officer
Hill International, Inc.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.