

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

HILARY HIGGINS
hhiggins@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

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

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

November 2, 2023

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

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

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for The Hilb Group Operating Company, LLC ("Hilb"), located at 6227 Executive Boulevard, Rockville, Maryland 20852, and write to inform you of a data security incident. By providing this notice, Hilb does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or about January 10, 2023, Hilb discovered suspicious activity related to several employee email accounts. Upon discovery, Hilb took immediate action to address and investigate the event, which included engaging third-party specialists to assist with determining the nature and scope of the event. A thorough investigation determined that an unauthorized actor gained access to employee email accounts for a limited period of time between December 1, 2022, and January 12, 2023. Hilb then began a thorough review of the contents of the email accounts in order to determine the type(s) of information contained within the accounts and to whom that information related. On July 28, 2023, the review was completed, and Hilb immediately began working to locate address information. On October 9, 2023, Hilb discovered that information related to seven hundred thirty-seven (737) residents of Maryland may have been accessed by an unauthorized party in connection with this incident. The information was limited to first and last name in combination with Social Security number, Driver's License number/ID, financial account information, medical information, and/or health insurance information.

On November 2, 2023, Hilb sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland law. The notice letters included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letters sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

Very truly yours,


Hilary Higgins, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A

The Hilb Group Operating Company LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



000010102G0500

P

RE: Notice of Data Breach

November 2, 2023

Dear [REDACTED]:

The Hilb Group Operating Company, LLC (“Hilb”) is writing to inform you of a potential data security event experienced by our company that may have involved your information as described below. We take the privacy and security of all information in our care seriously and are providing information about the event and steps you can take to help protect your information.

What Happened: On or about January 10, 2023, we discovered suspicious activity related to several employee email accounts. Upon discovery, we took immediate action to address and investigate the event, which included engaging third-party specialists to assist with determining the nature and scope of the event. A thorough investigation determined that an unauthorized actor gained access to employee email accounts for a limited period of time between December 1, 2022 and January 12, 2023. We then began a thorough review of the contents of the email accounts in order to determine the type(s) of information contained within the accounts and to whom that information related. On July 28, 2023, this review was completed, and we immediately began working to locate address information. On October 9, 2023, we completed our address review and we worked to provide potentially impacted individuals with this notification.

What Information Was Involved: The types of information that may have been contained within the email account includes your first and last name, in combination with the following data element(s): Social Security Number.

What We Are Doing: We have taken the steps necessary to address the event and are committed to fully protecting all of the information entrusted to us. Upon learning of this event, we immediately took steps to secure the email accounts and undertook a thorough investigation. We have also implemented additional technical safeguards to further enhance the security of information in our possession and to prevent similar incidents from happening in the future. Additionally, we are offering you complimentary credit monitoring and identity protection services.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, including activating the complimentary credit monitoring and identity protection services we are offering.

For More Information: Should you have any questions or concerns, we can be reached at 1-833-644-0798 between the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday, excluding holidays. The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

Jason S. Angus
Chief Operating Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring 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 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.



How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/hilbgroup> and follow the instructions provided. When prompted please provide the following unique code to receive services:



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 www.transunion.com	Experian 1-888-397-3742 www.experian.com	Equifax 1-888-298-0045 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; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. The Hilb Group may be contacted at 6227 Executive Blvd., Rockville, MD 20852.

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 1069 Rhode Island residents 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>. The Hilb Group may be contacted at 6227 Executive Blvd., Rockville, MD 20852.