McGuireWoods LLP
Gateway Plaza
800 East Canal Street
Richmond, VA 23219-3916
Phone: 804.775.1000
Fax: 804.775.1061
www.mcguirewoods.com

Janet Peyton
Direct: 804.775.1166

McGUIREWOODS

jpeyton@mcguirewoods.com
Fax: 804.698.2230

October 30, 2023

VIA EMAIL: idtheft@oag.state.md.us
The Honorable Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Notice of Data Breach

Dear Attorney General Brown:

I am writing on behalf of The Hilb Group LLC ("Hilb" or the "Company") with its headquarters located at 6802 Paragon Place, Suite 200, Richmond, Virginia 23230, to provide a report of a recent data breach. Hilb is an insurance broker. Hilb uses the Dayforce human capital management software ("Dayforce"), which is provided by Hilb's vendor Ceridian Dayforce Corporation ("Ceridian"), for Hilb's human resource functions. It is our understanding that a threat actor set up a fake website imitating the Dayforce login page, so that employees who searched for it on the internet (rather than clicking on the links provided internally by Hilb) would find the fake website instead and input their credentials. In so doing, the threat actor was able to gather credentials without breaching Hilb's server or network at all. On October 15, 2023, the threat actor successfully accessed the Dayforce account of a Hilb employee who is a Maryland resident and altered the employee's direct deposit information to attempt to redirect the employee's Hilb paycheck funds to the threat actor. Hilb learned of this issue when the employee notified Hilb of the suspicious alert the employee received from Ceridian about the employee's Dayforce account information being changed. The incident was then quickly resolved on October 15, 2023.

So far, there is no evidence that any personal information was exfiltrated or otherwise removed from the employee's Dayforce account, but it does appear that the threat actor had access to it. We do know that they at least had access to the employee's direct deposit information. Further, as a result of accessing this employee's account, the threat actor also had access to personal information for four (4) adult dependents of this employee, all of whom are also Maryland residents. Hilb has no indications that any of the employee's or the employee's dependents' personal information has been used for fraudulent purposes, other than the threat actor's failed attempt at redirecting funds, nor are we aware of any resulting identity theft, fraud, or financial losses. Ceridian is also currently unsure whether the threat actor accessed any other part of the employee's Dayforce account, but Ceridian is monitoring the dark web for

information related to this and similar incidents involving other Dayforce accounts. Again, while Hilb does not know whether the employee's or the employee's dependents' personal information was in fact accessed or used for any unauthorized purpose, other than the threat actor's attempt to redirect funds, Hilb is sending the impacted employee and each of their dependents written notice as a precautionary action.

This incident impacted five (5) Maryland residents. The personal information potentially disclosed for the employee in the incident included: name, date of birth, Social Security number, address, business and mobile phone numbers, business and personal email addresses, bank account name, routing, and account numbers, National Producer Number, and Dayforce employee ID number. The personal information potentially disclosed for the employee's dependents included: name, date of birth, and Social Security number. Formal, written notices are being sent to the impacted individuals on October 31, 2023.

Hilb has taken actions to mitigate the incident, including working with the impacted employee and Dayforce to successfully lock out the threat actor from the employee's Dayforce account. In addition, the Company is offering the impacted individuals a complimentary 12-month membership to Kroll's Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration services.

A copy of the template form of the notification letter that is being sent to the affected Maryland residents is included with this notice. As you will see, among other things, the letter (i) describes various steps the affected individuals can take to protect herself, (ii) provides contact information for consumer reporting agencies and relevant governmental agencies, and (iii) provides information about enrolling in 12 months of credit monitoring services, which the Company is offering to the affected individual at no cost.

If you have any questions about the information provided in this letter, or this incident generally, please feel free to contact me at the email or phone numbers listed above.

Sincerely,

Janet P. Peyton

Enclosures: Template Form Notification Letter

October 31, 2023

[redacted]
MD [redacted]

RE: Notice of Data Breach

Dear [redacted]:

I am writing to you on behalf of The Hilb Group LLC ("Hilb" or the "Company") with important information about a data security incident that recently occurred. Hilb takes the protection and proper use of your personal information very seriously. We are, therefore, contacting you to explain the incident and provide you information about security measures you can take to protect yourself and your personal information.

What Happened:
Hilb uses the Dayforce human capital management software ("Dayforce"), which is provided by our vendor Ceridian Dayforce Corporation ("Ceridian"), for Hilb's human resource functions. As you are aware, on October 15, 2023, your Dayforce account was compromised. Specifically, a threat actor successfully accessed your Dayforce account and altered your direct deposit information to attempt to redirect your Hilb paycheck funds to the threat actor. Hilb learned of this issue when you notified us of the suspicious alert you received from Ceridian about your Dayforce account information being changed. The incident was then quickly resolved on October 15, 2023.

What Information Was Involved:
So far, there is no evidence that any personal information was exfiltrated or otherwise removed from your Dayforce account, but it does appear that the threat actor had access to it. We do know that they at least had access to your direct deposit information, and potentially to other personal information including your name, date of birth, social security number, address, telephone, email, and Dayforce ID number. Your beneficiaries' personal information may also have been exposed and separate notifications are being sent to each impacted individual. Hilb has no indications that any of your personal information has been used for fraudulent purposes, other than the threat actor's attempt at redirecting funds, nor are we aware of any resulting identity theft, fraud, or financial losses. Ceridian is also currently unsure whether the threat actor accessed any other part of your Dayforce account, but Ceridian is monitoring the dark web for information related to this and similar incidents involving other Dayforce accounts. Again, while we do not know whether your personal information was in fact accessed or used for any unauthorized purpose, other than the threat actor's attempt to redirect funds, we are sending you this notice as a precautionary action.

What We Are Doing:
We have taken actions to mitigate the incident, including working with you and Dayforce to successfully lock out the threat actor from your Dayforce account.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. 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, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com/redeem** to activate and take advantage of these services.
*You have until **December 31, 2023** to activate your identity monitoring services.*
Activation Code: [redacted]
Verification ID: [redacted]

Additional information describing your services is included with this letter.

What You Can Do:
Please review the "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. You should also report any suspected incident of identity theft to law enforcement, and you can obtain a copy of any resulting police report. If you do suspect that you have been the victim of identity theft, you should also notify your state Attorney General and the FTC.

For More information:
If you have questions about this incident, please call **804-220-8899** Monday through Friday from 9:00 a.m. to 5:00 p.m. Eastern Time.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Rob Patton
Senior Vice President – Human Resources

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 Maryland residents: You may obtain one or more 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.

ChexSystems
If your bank account information was involved in the incident, you may place a security alert and/or security freeze with ChexSystems by visiting https://www.chexsystems.com or calling (800) 428-9623.

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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.

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.