BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

CHASE NORTH TOWER
450 LAUREL STREET
21ST FLOOR
BATON ROUGE, LOUISIANA
70801

PHONE: 225.381.7000
FAX: 225.343.3612

www.bakerdonelson.com

LAYNA RUSH, SHAREHOLDER
Direct Dial: 225.381.7043
Direct Fax: 225.382.0243
E-Mail Address: lrush@bakerdonelson.com

January 5, 2024

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

Re: *Vector Consulting, Inc - Notice of Breach by Third Party Vendor*

Dear Attorney General Brown:

I serve as outside counsel to Vector Consulting, Inc. ("Vector"), whose principal place of business is located 6455 E. Johns Crossing, Suite 250, Duluth, Georgia 30097.[1]

On December 26, 2023, Vector received communications from its third-party payroll vendor, Paycor, indicating that Paycor had been impacted by the MOVEit Transfer Cyber Vulnerability and that data related to some Vector employees may have been affected. According to Paycor, on May 31, 2023, Progress Software announced that it had discovered a previously unknown "zero-day" cyber vulnerability in its MOVEit Transfer software and that Paycor was impacted by the vulnerability. On December 26, 2023, Vector also received a list of potentially impacted employees and their data from Paycor. Because it appears that Paycor is notifying its customers and not the potentially impacted individuals, Vector determined to notify its employees of the incident and offer them complimentary identity theft protection and credit monitoring.

Notification letters were sent to impacted individuals on January 5, 2023 including a notification letter to four Maryland residents. The Maryland residents were offered one year of credit monitoring and identity theft protection. The personally identifiable information ("PII") that was potentially at risk included names and Social Security numbers.

---

[1] By providing this notice, Vector does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

The Maryland resident received notification that included:

- A description of the security event;
- Steps taken to mitigate any potential harm to consumers;
- Instructions for activation of 1 year of free identity theft protection services that include credit monitoring and a $1 million insurance reimbursement policy;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this event.

Vector is fully committed to protecting the privacy and the confidentiality of its employees' personal information. We will follow-up this correspondence with any forms or other documents that may need to be completed. Please contact me if you require any additional information regarding this incident.

Sincerely,

BAKER, DONELSON, BEARMAN, CALDWELL & BERKOWITZ, PC

By: Layna C. Rush
Layna C. Rush

Enclosure:

Sample Notification Letter sent to 4 residents.

Vector Consulting
Mail Handling Services
777 E. Park Dr.
Harrisburg, PA 17111

Re: Notice of Security Incident

January 05, 2024

Dear

Vector Consulting, Inc. ("Vector") values and respects the privacy and security of its employees' information, which is why we are notifying you of a security incident of which we were notified by our third-party payroll vendor, Paycor. This letter contains information regarding the incident and steps you can take to further protect your information should you feel that it is appropriate to do so.

What Happened? On December 26, 2023, Vector received communications from its third-party payroll vendor, Paycor, indicating that Paycor had been impacted by the MOVEit Transfer Cyber Vulnerability and that data related to some Vector employees may have been affected. According to Paycor, on May 31, 2023, Progress Software announced that it had discovered a previously unknown "zero-day" cyber vulnerability in its MOVEit Transfer software and that Paycor was impacted by the vulnerability. Paycor indicates that it immediately took steps to address the incident, including launching a forensic analysis with the assistance of outside experts, and that based on the analysis, the incident's scope was limited to the MOVEit Transfer platform. Paycor also states that the analysis included identifying the Paycor customers whose data may have been exposed as a result of the incident. Paycor indicated that the analysis was completed on October 20, 2023.

What Information Was Involved? On December 26, 2023, Vector received a list of potentially impacted employees and their data from Paycor. According to Paycor, the information that may have been impacted included your name, social security number and date of birth.

What Are We Doing? We are committed to protecting our employees' personal information. Because it appears that Paycor is notifying its customers and not the potentially impacted individuals, we are notifying you of this incident and offering you complimentary identity theft protection and credit monitoring through Experian. These services will be available to you for one (1) year at no cost to you to give you peace of mind. This letter contains additional information regarding these services and instructions on how you may activate the complimentary identity theft protection and credit monitoring. You must complete the activation steps listed on the next page.

What Can You Do? We recommend that you activate your complimentary credit monitoring and identity theft protection. In addition to activating the complimentary credit monitoring and identity theft protection, it is always a best practice to monitor your credit reports and financial statements routinely to ensure there is no suspicious activity. We have included additional information in this letter on steps you can take to protect your information if you so choose.

For More Information or if you have additional questions regarding the information contained in this letter, please call our Human Resources Department at 678-578-8931. We regret any inconvenience that this incident might have caused you.

Sincerely,

Manbir Khurana, CEO

STEPS YOU CAN TAKE

Below is information on steps you can take to protect yourself.

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**:

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-288-8057** by Be prepared to provide the engagement number as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-288-8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Below are additional actions you may take if you feel it is necessary.

➢ **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 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. Note that a security freeze generally does not apply to existing account relationships and when 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. There is no charge to place or lift a security freeze.

To place a security freeze on your credit report, contact each of the three major consumer reporting agencies using the contact information listed below:

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES		
Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security number, and date of birth;
- If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
- 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.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

➢ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, 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, which is an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.

➢ **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS, & REPORT FRAUD.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)

➢ **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

➢ **POLICE REPORT.** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it.

➢ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. The Federal Trade Commission also provides information at www.ftc.gov/idtheft. The FTC can be reached by phone: 1 - 877-438-4338; TTY: 1-866-653-4261 or by writing: 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Your State Attorney General also may provide information. For North Carolina residents: You may contact 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.

➢ **FILE YOUR TAXES QUICKLY AND SUBMIT IRS FORM 14039.** If you believe you are at risk for taxpayer refund fraud, the IRS suggests you file your income taxes quickly. Additionally, if you are an actual or potential victim of identity theft, the IRS suggests you give them notice by submitting IRS Form 14039 (Identity Theft Affidavit). This form will allow the IRS to flag your taxpayer account to alert them of any suspicious activity. Form 14039 may be found at https://www.irs.gov/pub/irs-pdf/f14039.pdf.

➢ **FAIR CREDIT REPORTING ACT.** You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Please note that identity theft victims and active-duty military personnel may have additional rights under the FCRA.

➢ **PROTECT YOURSELF FROM PHISHING SCAMS.** Learn to recognize phishing emails. Do not open emails from unknown senders and be sure not to click on strange links or attachments. Never enter your username and password without verifying the legitimacy of the request by contacting the sender by telephone or other methods. Replying to the email is not a safe way to confirm. Visit https://www.consumer.ftc.gov/articles/0003-phishing for more information on these types of scams.