



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 14, 2024

VIA E-MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent PVE, LLC (“PVE”) located at 2000 Georgetown Drive, Suite 101, Sewickley, Pennsylvania 15143, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. By providing this notice, PVE 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.

Nature of the Data Event

PVE became aware that certain systems within its network were inaccessible and immediately undertook efforts to secure its systems and begin an investigation. The investigation determined there was unauthorized access to PVE’s network between February 19, 2024, and March 4, 2024, and during this time certain files were copied. PVE reviewed the files and systems to determine their content and to whom they were related. Through this process PVE identified personal information as defined by state law including name and Social Security Number. The review also determined that other types of sensitive information may have been present in the system at the time of the event if provided to PVE in the course of the onboarding and/or benefits administration process including date of birth, driver’s license or state identification number, passport number, Green Card, and/or medical information.

Notice to Maryland Resident

On or about June 14, 2024, PVE provided written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the activity, PVE moved quickly to investigate and respond, assess the security of PVE systems, and identify potentially affected individuals. PVE has security measures in place to protect information in its care and is also evaluating policies, procedures, and technical security measures and implementing additional safeguards to further secure the information in its systems. PVE is providing access to credit monitoring services for one (1) year, through Transunion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, PVE is providing individuals with guidance on how to better protect against identity theft and fraud. PVE is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

PVE also notified federal law enforcement of this incident and is providing written notice of same to relevant state regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/kzf
Attachment

EXHIBIT A

PVE, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



June 7, 2024

Dear [REDACTED]:

PVE, LLC ("PVE") writes to inform you of an incident that may involve some of your information. This letter provides an overview of the incident, our response to it, and steps you may take to protect your information, should you feel it is appropriate to do so.

What Happened? We became aware that certain systems within our network were inaccessible. In response, we immediately undertook efforts to secure the systems and investigate what occurred. The investigation determined there was unauthorized access to our network between February 19, 2024, and March 4, 2024, and during this time certain files were copied. We reviewed the involved systems and files to identify the contents to whom they relate and on April 22, 2024, we completed our review.

What Information Was Involved? The investigation determined that your name and Social Security number were present in an involved system at the time of the incident, as well as the following types of information to the extent it was provided to PVE Human Resources in the course of the onboarding and/or benefits administration process: date of birth, driver's license or state identification number, passport number, Green Card, and medical information.

What We Are Doing. The confidentiality, privacy, and security of information within our care are among our highest priorities. Upon learning of the accessibility issues, we moved quickly to investigate and respond. The investigation actions included steps to access and secure our network and continue our normal business operations, review the involved systems and files, and notify potentially impacted individuals. We also reported this event to federal law enforcement.

PVE has an ongoing commitment to safeguarding the privacy and security of information provided to us. As part of that commitment, we implemented additional security measures within our network and completed a review of our policies and procedures to further secure the information in our systems.

As an added precaution, we are also offering you 12 months of credit monitoring and identity restoration services at no cost to you through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Details of the services offered and instructions on how to enroll may be found in the *Steps You Can Take to Protect Personal Information* section of this letter.

000010102G0400

P

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. You may review the *Steps You Can Take to Protect Personal Information* section of this letter for useful information on what you can do to better protect against possible misuse of information. You may also enroll in the complimentary credit monitoring services we have provided for you. Please note, due to privacy restrictions, we are unable to automatically enroll you in these services.

For More Information. If you have questions, you can call our dedicated assistance line at 1-800-405-6108 Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays). You may also write to PVE at 2000 Georgetown Drive, Suite 101, Sewickley, Pennsylvania 15143.

Sincerely,

PVE, LLC

Steps You Can Take to Protect Personal Information

Enroll in Credit Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: **62BA2100DF6C**

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 Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers 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 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 a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s 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 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); 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:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

As a best practice, consumers should change all passwords to their personal accounts on a regular basis, use strong passwords, and refrain from using the same password for multiple accounts. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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 reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There is approximately 1 Rhode Island resident that may be impacted by this event.