

# **EXHIBIT A**

VPS of MI., PLLC.  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998



November 15, 2024

## NOTICE OF SECURITY INCIDENT

VPS of MI., PLLC (“VPS”) writes to notify you of an incident that may affect the privacy of some of your information. This letter provides you with details about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

**What Happened?** On June 4, 2024, VPS detected irregular activity within our computer network. VPS launched an investigation and determined that our server had been infected with malware, which prevented access to certain files on our server. Through our investigation, we also determined that an unauthorized actor exfiltrated information from our server.

**What Information Was Involved?** The following information was potentially exfiltrated from our network, if you supplied it to VPS: your name, Social Security number, and/or driver’s license number. In addition, the following medical information was potentially exfiltrated, if part of your VPS medical record: medical history information, mental or physical condition or diagnosis by a health care professional, medical treatment information, disability information, prescription information, and medical record number. If part of our records, the following information related to your health insurance was also potentially exfiltrated: health insurance policy number; subscriber number; any medical information in an individual’s health insurance application and claims history, including any appeals records; and health insurance group or plan number. At this time, VPS is not aware of any actual or attempted misuse of your information in connection with this incident.

**What We Are Doing.** Data privacy and security are among VPS’ highest priorities, and there are extensive measures in place to protect information in VPS’ systems. Upon discovery, VPS promptly commenced an investigation and notified law enforcement of this incident. As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our policies, procedures, and processes related to the storage and access of personal information to reduce the likelihood of a similar future event. We are also notifying applicable regulatory authorities, as required by law.

As an added precaution, we are also offering twelve (12) months of complimentary access to credit monitoring services through Cyberscout, a TransUnion company. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

**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 free credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. There you will also find more information regarding the complimentary credit monitoring services we are making available to you. While VPS will cover the cost of these services, you will need to enroll yourself in the services we are offering, if you would like to do so.

000010102G0400

P

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 1-844-509-4070 or you may also write to VPS at 31500 West 13 Mile Road, Suite 100, Farmington Hills, MI, 48334.

Sincerely,

VPS OF MI., PLLC

## STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

### Enroll in 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 the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation 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:

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.

00001020280000

### Monitor Your 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 a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

P

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
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**

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](http://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 the relevant state Attorney General. This notice has not been delayed by law enforcement.

*For Massachusetts residents*, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.