SIDLEY

SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
+1 202 736 8000
+1 202 736 8711 FAX

AMERICA • ASIA PACIFIC • EUROPE

+1 202 736 8465
CTBROWN@SIDLEY.COM

February 2, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Via email – Idtheft@oag.state.md.us

Re: Notice of Data Security Incident Impacting Vehicle Service Group

Dear Attorney General Brian Frosh:

We are writing to inform you about a data security incident that may have affected personal information maintained by Vehicle Service Group ("VSG"). This includes the information of approximately 2 individuals who are Maryland residents.

VSG recently confirmed a data security incident involving certain VSG information. VSG began investigating a potential data theft incident on December 15, 2021, after anonymous individuals claimed to have access to company information. VSG took prompt action to secure its systems, report the incident to law enforcement, and investigate the matter.

On January 27, 2022, VSG concluded that the incident may have impacted personal information related to 2 Maryland residents. VSG has not been able to confirm that personal information of each of these individuals has been compromised in this incident. But out of an abundance of caution, VSG is notifying all current employees, as well as certain former employees going back over a decade, of Vehicle Service Group LLC employed in Madison, IN and all in Downers Grove, IL or who are remote employees reporting into those locations to inform them of the incident. Information available in the affected files might have included, in part or whole, employee's name, contact information, date of birth, Social Security number, driver's license number or other government issued identification numbers, financial account information, demographic information, salary, tax, insurance and other benefits information, and other HR information associated with one's employment.

On February 2, 2021, VSG is providing notification to approximately 1,180 individuals, including approximately 2 Maryland residents, because their personal information may have been affected. The privacy and security of personal information is of utmost importance to VSG. As soon as VSG discovered this incident, its IT security team took prompt steps to investigate the incident and strengthen the security of its systems. VSG has also arranged to provide affected individuals with tools for credit monitoring, fraud detection, and identity restoration at no cost for two years through Experian.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Colleen Theresa Brown

Colleen Theresa Brown
Partner

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 2, 2022

H4834-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

[Variable Header - CA Only]

Dear Sample A. Sample:

We are writing to let you know about a data security incident involving your personal information, the steps we are taking, and the resources we are making available to you.

What Happened?

We recently confirmed a data security incident involving certain Vehicle Service Group ("VSG") information. We began investigating a potential data theft incident on December 15, 2021, after anonymous individuals claimed to have access to company information. We took prompt action to secure our systems, report the incident to law enforcement, and investigate the matter. We are providing this notice to you because your information was available through the impacted VSG files.

What Information Was Involved?

Information available in the affected files might have included, in part or whole, your name, contact information, date of birth, Social Security number, driver's license number or other government issued identification numbers, financial account information, demographic information, salary, tax, insurance and other benefits information, and other HR information associated with your employment. If you maintained password information for business or personal accounts in the VSG files, those passwords may also have been included in the affected files.

What We Are Doing

The privacy and security of your personal information is of utmost importance to us. As soon as we discovered this incident, our IT security team took prompt steps to investigate the incident and strengthen the security of our systems. We have also arranged to provide you tools for credit monitoring, fraud detection, and identity restoration at no cost for two years through Experian.

To help protect your identity, we are offering a complimentary 24-month 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**: **May 31, 2022** (Your code will not work after this date.)*
- ***Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/3bcredit***
- *Provide your **activation code**: **ABCDEFGHI***

0000001

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 (888) 397-0050 by ***May 31, 2022.*** *Be prepared to provide engagement number* ***B026263*** *as proof of eligibility for the identity restoration services by Experian.*

Additional details regarding your 24-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.*

What You Can Do

We recommend that you remain vigilant by reviewing your account statements, monitor free credit reports, and review the enclosed "Additional Ways to Protect Your Identity: Important Identity Theft Information". If you had stored your personal or business passwords in unencrypted (not password-protected) files on the VSG servers, you are urged to change those passwords as soon as possible (using a completely new and unique format). Please note you should not store passwords, personal or business-related, in unencrypted Word / Excel or other file types. Consider using a password generator and vault to properly secure your passwords.

For More Information

If you have further questions or concerns, you can find more information by calling (888) 397-0050.

We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

Jim Zoretich

Jim Zoretich
President, Vehicle Service Group

* 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.

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some we suggest you consider:

Reviewing Your Accounts and Credit Reports
Federal regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-800-888-4213
Equifax.com	Experian.com	Transunion.com

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert
A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report. If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report
A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge. If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze, and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft
If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to educate yourself, identity theft victims, and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of Iowa, Maryland, Massachusetts, North Carolina and Oregon

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their website at http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their website at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.