

JacksonLewis

Jackson Lewis P.C.

100 South Ashley Drive, Suite 2200
Tampa, FL 33602
(813) 512-3210
(813) 512-3211 Fax
jacksonlewis.com

MY DIRECT DIAL IS: (813) 512 3225

MY EMAIL ADDRESS IS: JOSEPH.LAZZAROTTI@JACKSONLEWIS.COM

November 1, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Data Breach Notification

Dear Attorney General Brown:

Please be advised¹ that on August 27, 2024, our client, Van Wagner Group, LLC, located at 800 3rd Ave., NY, NY 10022 (“Company”) learned that its systems had been compromised as a result of a malware attack (“Incident”). Based on the investigation to date, it appears the Incident occurred between August 3, 2024 and September 4, 2024.

The Company experienced a malware attack. Root cause was not confirmed but may have been carried out through a VPN interface. The Company discovered the Incident may have affected personal information on August 27, 2024, but did not identify the compromised files until September 9, 2024. It then needed to review those files to identify the individuals whose personal information may have been impacted. The notification process included arranging for notification, confirming address data, engaging a call center, and extending ID theft and credit monitoring services, as well as evaluating notification requirements across many states.

The personal information that may have been involved in the Incident included personal information such as name, address, email address, date of birth, and Social Security number. The Company believes a total of 5354 individuals were affected based on its investigation to date, including 126 residents of Maryland. Immediately upon discovering the Incident, the Company took steps to determine its scope and who was affected. The Company engaged third-party forensics experts to examine the Company’s systems to assist in determining the full scope of the information at risk. The Company has notified potentially affected individuals on October 31, 2024. A draft copy of the notification is attached.

¹ Please note that by providing this letter the Company is not agreeing to the jurisdiction of the State of Maryland, or waiving its right to challenge jurisdiction in any subsequent actions.

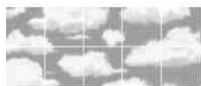
As set forth in the attached letter, the Company has taken numerous steps to protect the security of the personal information of the affected individuals and mitigate any harm, including providing 12 months of credit monitoring and ID theft protection services at no cost. To help ensure an incident like this will not occur in the future, the Company has taken several steps including changing system passwords, strengthening system authentication and firewall security, adding new tools that can help detect and stop future attacks, and improving system monitoring. Should the Company become aware of any significant developments concerning this situation, we will inform you.

Sincerely,

JACKSON LEWIS PC

Joseph J. Lazzarotti

Encl.



Van Wagner

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Notice of Data Breach

Dear <<Full Name>>,

We recently experienced a data incident which may have resulted in unauthorized access or acquisition of your personal information. We are sending this notice to you to provide information about the incident, and to let you know that we are not aware of any improper use of your personal information. We apologize for any inconvenience this may cause you.

What Happened

On August 27, 2024, we discovered a data incident which may have involved your personal information as the result of malware attack which occurred on August 3, 2024.

What Information Was Involved

The data elements involved may have included names, addresses, dates of birth, email addresses, and Social Security numbers.

What We Are Doing

Upon discovering the incident, we commenced an investigation working with our internal response team and our third-party IT service providers to secure our information systems and contain the effects of the incident. We also arranged to make available ID theft and credit monitoring services, as well as other steps to protect your personal information.

We treat all personal information in a confidential manner and are proactive in the careful handling of such information. Theft of data and similar incidents are difficult to prevent in all instances. We have reviewed our systems, and we are making improvements where we can to minimize the chances of this happening again. For example, we have changed system passwords, strengthened system authentication and firewall security, added new tools that can help detect and stop future attacks, and improved system monitoring.

What You Can Do

While we are unaware of any misuse of personal information as a result of this incident, we outline below steps you can take to protect your identity and personal information.

In addition, we are offering identity theft protection services through Equifax Credit Watch™ Gold at no cost to you. These identity theft protection services include <<CM Duration>> months of identity theft recovery services and credit monitoring. With this protection, you will have access to resources to help you resolve issues if your identity is compromised. We encourage you to contact Equifax with any questions and to enroll in these services by going to www.equifax.com/activate and using the Enrollment Code <<Code>>. Please note that you must enroll within 90 days of the date of this letter.

For More Information

If you have questions or concerns, you should contact the call center we established to assist you by calling **855-277-9026**. You also may contact Liza Villafane at Van Wagner, via email at lvillafane@vanwagner.com; or by phone at 212-699-8459. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

Liza Villafane
Senior Vice President, Human Resources

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

- Order Your Free Credit Report at www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any.
- Place a Fraud Alert on Your Credit File. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

Equifax, P.O. Box 740241, Atlanta, GA 30374, 1-888-685-1111, www.equifax.com,

Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com,

TransUnion, P.O. Box 2000, Chester, PA 19016, 1-800-916-8800, www.transunion.com,

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
- The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.
- The IRS also offers Identity Protection: Prevention, Detection and Victim Assistance which can be found at: <https://www.irs.gov/Individuals/Identity-Protection>.
- *For District of Columbia Residents:* You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov.
- *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, <https://www.marylandattorneygeneral.gov>

- *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act> or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to <https://www.sos.nm.gov/cybersecurity/tips-for-new-mexicans/>
- *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/>; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
- *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.
- *For Rhode Island Residents:* You can obtain information from the Rhode Island Attorney General about steps you can take to help prevent identity theft at: 150 South Main Street, Providence, RI 02903, (401) 2744400, www.riag.ri.gov. Thirteen Rhode Island residents' data was involving in the incident.