JacksonLewis

Jackson Lewis P.C.
200 Connell Drive, Suite 2000
Berkeley Heights NJ 07922
(908) 795-5200 Main
(908) 464-2614 Fax
jacksonlewis.com

Via Regular Mail and Email

June 30, 2023

Email:DOJ-CPB@doj.nh.gov
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification

Dear Attorney General :

On behalf of our client, Valley Power Systems, Inc. ("Valley")[1], we are writing to provide information regarding a cyber attacked experienced by Valley that may have resulted in the unauthorized disclosure of personal information (the "Incident").

On June 9, 2023, Valley discovered that personal information may have been accessible to an unauthorized actor(s) as a result of the Incident. As a result, our client immediately began its investigation of the Incident and determined that the Incident occurred sometime on or around June 9, 2023.

Valley has determined at this point in its investigation that the personal information of certain Valley employees (including related affiliates), and their dependents, may have been disclosed to the unauthorized party as a result of the Incident. The personal information may have included . Based on our investigation to date, we believe one (1) resident of the state of New Hampshire was impacted by the Incident.

Valley has been in contact with law enforcement, including the Federal Bureau of Investigation ("FBI"), and are supporting law enforcement's investigation. This communication was not delayed at the request of law enforcement.

To protect against an incident like this from reoccurring, Valley worked with its information technology team in an effort to ensure the Incident did not result in any additional exposure to personal information and took steps to confirm the integrity of Valley's systems.

Valley will be making credit monitoring and ID restoration protection services available at no cost to potentially affected persons. For persons who timely enroll, these services will be available for . Additionally, Valley began mailing notices to affected individuals on June 30, 2023.

[1] Valley's corporate address is 425 S. Hacienda Blvd., City of Industry, CA 91745. Valley also provides administrative support to related entities.

Valley has taken numerous steps to protect the security of the personal information of the affected individuals. To help ensure an incident like this will not occur in the future, Valley is reviewing its policies and procedures to make sure employees are reminded about best practices on data security.

If you require any additional information on this matter, please do not hesitate to contact me.

Very truly yours,

JACKSON LEWIS PC

Joseph J. Lazzarotti
Rob Yang

Encl.

[Company Logo] [Date]

[Recipient's Name]
[Address]
[City, State, Zip]

Dear [Name]:

At Valley Power Systems, Inc., we value and respect the privacy of your information, which is why we are writing to inform you we recently learned that some of your personal information may have been subject to unauthorized access or acquisition as the result of a cyberattack (the "Incident"). While we are not aware of any misuse of your information, we are providing this notice to inform you of the Incident and to call your attention to steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened?
On June 9, 2023, we discovered your personal information may have been accessible to an unauthorized actor(s) as a result of the Incident. Based on the investigation, it appears the Incident occurred sometime on or around June 9, 2023.

What Information Was Involved?
The following types of data may have included personal information such as

.

What We Are Doing.
Valley Power Systems, Inc. takes this Incident and the security of your personal information very seriously. Upon learning of this incident, we launched an in-depth investigation to determine the scope of the Incident and identify those potentially affected. This included working with our information technology team in an effort to ensure the Incident did not result in any additional exposure to personal information and taking steps to confirm the integrity of our systems. We also reported the Incident to the federal authorities. This communication was not delayed at the request of law enforcement. As an added precaution, we are also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services. If you wish to receive these services, activation instructions are below.

What You Can Do.
The attached sheet describes steps you can take to protect your identity, credit and personal information. We are also offering identity theft protection services through TransUnion at no cost to you. These identity theft protection services include of identity theft recovery services and credit monitoring. With this protection, TransUnion will help you resolve issues if your identity is compromised. We encourage you to contact First Watch Corporation with any questions and to enroll in these services by calling [insert toll-free line] any time between Monday - Friday 9:00 AM to 5:30 PM eastern, or going to and using the Enrollment Code [To be inserted]. Please note that you should enroll within 90 days of the date of this letter.

In addition to taking advantage of the credit monitoring and identity restoration services outlined above, set forth in the attached guide are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s).

For More Information.

We apologize for the inconvenience this may cause. We are committed to maintaining the security and privacy of personal information. We want you to be assured that we are taking steps to minimize the chances of a similar occurrence happening again. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at [Phone Number], Monday - Friday 9:00 AM to 5:30 PM eastern.

Regards,

[Name of Signatory]
[Title]
[Client Name]

ADDITIONAL RECOMMENDED STEPS

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. 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.

- 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	1-800-525-6285	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	1-800-680-7289	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.