Troutman Pepper Locke LLP
111 South Wacker Drive, Suite 4100
Chicago, IL 60606

troutman.com

Kenneth K. Suh
D 312.443.0640
F 312.896.6240
kenneth.suh@troutman.com

February 28, 2025

Maryland Attorney General Anthony G. Brown
Idtheft@oag.state.md.us

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

VIA EMAIL

Re: Power Test Notice pursuant to Maryland Code Commercial Law § 14-3501

Dear Attorney General:

We represent Power Test Industries, LLC ("Power Test"). Power Test is providing a notice pursuant to Maryland Code Commercial Law § 14-3501 of a cybersecurity incident that may have affected the personal information of residents of Maryland.

Number of Maryland Residents Affected by the Breach

The cybersecurity incident may have affected the personal information of 2 residents of Maryland. The personal information affected may include individuals' names, addresses, financial accounts, social security numbers, and other personal information of certain individuals.

What Happened

What Happened? Power Test experienced a network outage that was the result of a cybersecurity attack. In response, Power Test engaged Kroll, a leading cybersecurity firm, to help contain the attack, investigate the incident, and restore their systems in a safe manner. The investigation determined that on or around April 29, 2024 the individual potentially gained unauthorized access to certain files and folders that may have contained personal information.

To date, Power Test is not aware of any reports of identity fraud or improper use of the information as a direct result of this incident, and Power Test has no reason to believe that fraud or improper use will occur.

What Power Test is Doing

Power Test engaged a reputable law firm, who engaged third-party forensic analysis firm and a document review firm to analyze the contents of the impacted data. Power Test segregated the impacted data into two phases. Phase one data was prioritized due to its high probability of containing personal information and its relatively smaller size. Counsel notified Power Test of its notification obligations as to phase one on or around June 10, 2024 and the phase one individuals were notified on or around June 13, 2024. Phase two data was analyzed after phase one data due to its large size and low probability of containing personal information. Counsel notified Power Test of its notification obligations as to phase two on or around December 24, 2024 and the phase two individuals were notified on or around January 7, 2025. A small number of individuals were notified by substitute notification on February 7, 2025.

While Power Test does not believe that this incident has resulted in a significant risk of identity theft and it is not aware of any identity theft arising from this incident, Power Test is offering credit monitoring services for 1 year at no cost to the affected individuals.

* * * * *

Please do not hesitate to contact me with any questions related to this matter.

Sincerely,

Kenneth K. Suh

YOUR LOGO HERE

<<MemberFirstName>> <<MemberLastName>>

<<Address1>>

<<Address2>>

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

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information. The privacy and security of the personal information we maintain is of the utmost importance to Power Test Industries, LLC (“Power Test”). We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On April 29, 2024, Power Test experienced a network outage. We immediately initiated an investigation and determined that Power Test was under a cybersecurity attack. In response, Power Test engaged Kroll, a leading cybersecurity firm, to help contain the attack, investigate the incident, and restore our systems in a safe manner.

What information was involved?

Following an extensive review and analysis of the data involved in the attack, we determined that some of your personal information may have been impacted by this incident including, <<List of Personal Information>>.

What we are doing.

Although we are not aware of any circumstance in which personal information was misused as a result of this incident, to help relieve concerns and restore confidence following this incident, we have secured the services of Experian to provide IdentityWorks at no cost to you for <<ServiceTerminMonths>> months.

Visit **https://www.experianidworks.com/3bcredit** to activate and take advantage of your identity monitoring services.

Your activation code is: <<Activation Code>>.

You have until <<Activation Date>> to activate your identity monitoring services.

If you have questions or need assistance signing up, please contact Experian at 877.288.8057. Monday through Friday from 8 am – 8 pm CST (excluding major U.S. holidays). Please be prepared to provide your Engagement Number: <<Activation Code>>.

ADDITIONAL DETAILS REGARDING YOUR <<ServiceTerminMonths>>-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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Jim Miller, CEO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.