LEWIS BRISBOIS BISGAARD & SMITH LLP

David B. Sherman
500 E. Swedesford Road
Suite 270
Wayne, PA 19087
David.Sherman@lewisbrisbois.com
Direct: 215.977.4070

November 15, 2019

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

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Wayside Technology Group, Inc. ("Wayside"), located in Eatontown, New Jersey. This letter is being sent pursuant to N.H. Rev. Stat. §§ 359-C:19 - C:21 because we believe the personal information of one (1) New Hampshire resident may have been affected by a recent data security incident. The incident may have involved unauthorized access to resident's Social Security numbers, passport numbers, driver's license/state identification numbers, financial account information, medical/health information, and/or username and password.

On June 20, 2019, Wayside discovered unusual activity involving its email system. Upon learning of this activity, Wayside launched an internal investigation and retained a leading digital forensics firm to perform an independent investigation to determine what happened, whether any personal information had been accessed without authorization, and to identify the scope of individuals affected. On October 9, 2019, the forensic investigation first revealed that personal information of certain individuals may have been accessed without authorization, and the investigation continued in subsequent time to identify the full scope of individuals affected.

At present, the investigation has revealed one (1) resident of New Hampshire whose information may have been affected. Wayside has implemented additional security features to safeguard personal information in its possession and minimize the likelihood that an event like this could occur again in the future. Wayside notified the affected New Hampshire resident via the attached letter on November 15, 2019, and is providing twelve (12) months of complimentary credit and identity monitoring services through Kroll to all affected residents. Please feel contact me should you have any questions.

Sincerely,

David B. Sherman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter

CC: Sam Genovese (Lewis Brisbois Bisgaard & Smith, LLP, *via email*)

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Subject: Notice of Data Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident that may have involved your personal information. Wayside Technology Group, Inc. ("Wayside") takes the privacy and security of your information very seriously. This is why we are contacting you and informing you about steps that can be taken to help protect your personal information.

What Happened? On June 20, 2019, we discovered unusual activity involving our email system. Upon learning of this activity, we launched an internal investigation and retained a leading digital forensics firm to perform an independent investigation to determine what happened, whether any personal information had been accessed without authorization, and to identify the scope of individuals affected. On October 9, 2019, the investigation first revealed that personal information of certain individuals may have been accessed without authorization. While we are not currently aware of the misuse of any information as a result of this incident, we are sending you this letter to inform you of the incident and to share steps you can take to help protect your information.

What Information Was Involved? Based on our investigation, the information may include your Social Security Number, passport number, driver's license/state identification number, financial account information, medical health information, and username and password.

What Are We Doing? As soon as we discovered the incident, we took the steps discussed above. In addition, we have taken affirmative steps to minimize the likelihood of a similar incident occurring in the future. This includes working with leading cybersecurity experts to enhance the security of our digital environment. We are also providing you with information about steps that you can take to help protect your personal information.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **February 13, 2020** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. In addition, if you have not already done so, we encourage you to complete IRS Form 14039, Identity Theft Affidavit, which you can obtain at http://www.irs.gov/pub/irs-pdf/f14039.pdf. If you have other identity theft / tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. You should be especially aware of any requests, calls, emails, letters, or other questions about your family member's financial accounts or from individuals purporting to be from the IRS or other entities you would not be expecting contact from. If you receive any type of unexpected request for your family member's personal information, you should not provide that information and instead contact the organization to verify the request is legitimate.

For More Information: We remain committed to protecting your personal information and apologize for any worry or inconvenience this may cause you. If you have any questions, please contact Kroll at 1-877-514-0832, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below:

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.