Jennifer A. Coughlin
Office: 267-930-4774
Fax: 267-930-4771
Email: jcoughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 26, 2017

VIA E-MAIL AND FIRST CLASS U.S. MAIL
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Bentley Truck Services, Inc., headquartered at 7777 Essington Avenue, Philadelphia, Pennsylvania 19153, and are writing to notify your office of an incident that may affect the security of personal information relating to two (2) Maryland residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Bentley Truck Services, Inc. does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Nature of the Data Event

Bentley Truck Services, Inc. ("Bentley") was the targeted victim of an email spoofing attack on January 24, 2017, by an individual pretending to be Bentley's Owner. A request was made from what appeared to be a legitimate Bentley email address for all 2016 Bentley employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before the company discovered that the request was made from a fraudulent account by someone using the name and email address that appeared to be from Bentley's Owner. Bentley discovered the fraudulent nature of the request on January 24, 2017 and has been working tirelessly to investigate and to mitigate the impact of the attack.

Notice to Maryland Residents

On January 24, 2017, Bentley provided preliminary notice to current employees via email and work-place announcements. A copy of this notice is attached here as ***Exhibit A***. On January 26, 2017, Bentley will begin providing written notice of this incident to all affected current and former employees, which includes two (2) Maryland residents. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and to Be Taken

Upon discovering the fraudulent nature of the email, Bentley moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

Bentley is providing all potentially affected individuals access to 2 free years of credit and identity monitoring services, including identity restoration services, through Experian, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident.

Additionally, Bentley is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Bentley is also providing written notice of this incident to other state regulators as necessary. Bentley has provided notice of this incident to the IRS.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4774.

Very truly yours,

Jennifer A. Coughlin of
MULLEN COUGHLIN LLC

JAC:ncl

Enclosures

Exhibit A

MEMORANDUM

TO: Team Members Employed by Bentley Truck Services, Inc. ("Bentley") in 2016

DATE: January 24, 2017

RE: URGENT COMMUNICATION – Preliminary Notice of Data Incident

We recently discovered that our company was the targeted victim of an email spoofing attack on January 24, 2017, by an individual pretending to be the Owner. A request was made from what appeared to be a legitimate Bentley email address for all 2016 Bentley employee W-2 information. Unfortunately, copies of all 2016 employee W2 forms were provided before we discovered that the request was made from a fraudulent account by someone using the name and an email address that appeared to be from our Owner. We discovered the fraudulent nature of the request on January 24, 2017 and have been working tirelessly to investigate and to mitigate the impact of the attack.

Please note that this incident affects you only if you were employed by Bentley in 2016. If your employment did not begin with Bentley until 2017, then your information has not been impacted.

The confidentiality, privacy, and security of our employee information is one of our highest priorities. While our investigation is ongoing, we felt it important to notify you about this incident, and what we are doing to investigate and respond, as quickly as possible. Here are some actions that we are taking and that we encourage you to take:

- Identity Protection. As a precaution, for those individuals affected by this incident, we will be arranging for a vendor to protect your identity at no cost to you. The cost of this service will be paid for by Bentley and instructions for activating your protection will be sent to you shortly. ***We strongly encourage you to act to take advantage of these free identity protections services as soon as possible.*** It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.
- Notice to Affected Individuals. We also will be mailing information to all impacted current and former Bentley team members.
- Notice to Law Enforcement. We will be notifying any necessary state law enforcement and Attorneys General as well.
- Filing of 2016 Tax Returns. We encourage you to file your 2016 tax return as soon as possible, if you have not already done so. You can contact the IRS at http://www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.
- Information Technology Systems Review. At this time, we do not believe that our IT systems were otherwise compromised by this attack.
- Employee Training. Unfortunately, even the best technology cannot prevent all cyber-attacks, particularly those intended to fool employees into providing sensitive company

information. We will continue and improve upon our information security awareness and training programs for all employees.

We apologize for any inconvenience this incident causes you. Please know that we are working diligently to remedy this incident and to prevent any similar incidents from occurring in the future. If you have any questions about the contents of this notice or about the incident, please contact us Mike Napoliello at (215) 837-2954.

Exhibit B

BENTLEY
Truck Services, Inc.

NationaLease

January 26, 2017

«AddressBlock»

Dear «FIRST_NAME» «LAST_NAME»:

I am writing to make you aware of a recent email spoofing attack that may affect the security of your personal information. If you are a current employee of Bentley Truck Services, Inc. ("Bentley") you received a preliminary notice regarding this incident on January 24th or 25th, 2017. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? We recently discovered that our company was the targeted victim of an email spoofing attack on January 24, 2017, by an individual pretending to be our Owner. A request was made from what appeared to be a legitimate Bentley email address for all 2016 Bentley employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before we discovered that the request was made from a fraudulent account by someone using the name and an email address that appeared to be from our Owner. We discovered the fraudulent nature of the request on January 24, 2017 and since discovery have been working tirelessly to investigate and to mitigate the impact of the attack.

What Information Was Involved? A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent emails. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Bentley has stringent security measures in place to protect the security of information in our possession. At this time, we do not believe that the individuals who sent the fraudulent emails accessed our computer network or that our IT systems were otherwise compromised by this attack. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We have contacted the IRS and FBI and will be contacting the relevant state Attorneys General.

As an added precaution, we have arranged to have Experian protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice, and you can use them at any time during the next 24 months. The cost of this service will be paid for by Bentley. ***We strongly encourage you to act to take advantage of these free identity protection services as soon as possible.*** It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

307 HERON DRIVE	3053 ROUTE 73 SOUTH	7777 ESSINGTON AVENUE	244 QUIGLEY BOULEVARD	3555 NW 77th AVE., BLDG. A
LOGAN TOWNSHIP, NJ 08085	MAPLE SHADE, NJ 08052	PHILADELPHIA, PA 19153	NEW CASTLE, DE 19720	MIAMI, FL 33122
Office: 856-467-4446	Office: 856-320-2710	Office: 215-937-1044	Office: 302-328-4600	Office: 305-477-3031
Fax: 856-467-2455	Fax: 856-320-2719	Fax: 215-937-1005	Fax: 302-328-4601	Fax: 305-477-0325

www.bentleytruckservices.com

While Fraud Resolution assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through ProtectMyID® Elite as a two-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

1. Ensure that you **enroll by**: February 4, 2019 (Your code will not work after this date.)
2. **Visit** the ProtectMyID website to enroll: **www.protectmyid.com/enroll**
3. Provide your **activation code**: «EXPERIAN_CODE»

If you have questions about the incident, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please contact Experian's customer care team at 877-441-6943 by February 4, 2019. Be prepared to provide engagement number **PC106169** as proof of eligibility for the fraud resolution services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH PROTECTMYID MEMBERSHIP:

A credit card is **not** required for enrollment in ProtectMyID.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in ProtectMyID:

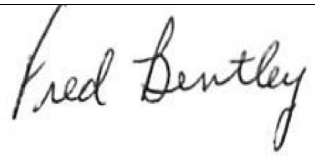
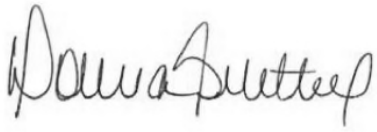
- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Scan:** Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts:** Alerts you of changes to your mailing address
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** Get help replacing credit, debit, and medical insurance cards.

What You Can Do. You can review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud". You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 tax return as soon as possible, and when you file, we also encourage you to file IRS Form 14039 (an identity theft affidavit) with your tax return.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call Mike Napoliello at (215) 837-2954.

Bentley takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

	
Fred Bentley President	Donna Bentley Chief Financial Officer

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, list, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement. This notice was not delayed by a law enforcement investigation.