LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

SIAN SCHAFLE
DIRECT DIAL: 215.977.4067
SIAN.SCHAFLE@LEWISBRISBOIS.COM

May 6, 2016

Via First Class US Mail
Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: **Notice of Data Event**

Dear Attorney General Foster:

We represent Digilant, 2 Oliver Street, Boston, MA, 02114, and are writing to notify your office of an incident that affects the security of personal information relating to one (1) New Hampshire resident. By providing this notice, Digilant does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On May 3, 2016, Digilant discovered that it was the targeted victim of an email spoofing attack. Through this attack, requests were made on March 30, 2016 for 2015 Digilant employee W-2 information from an individual or individuals purporting to be a Digilant senior executive. The 2015 Digilant employee W-2 information was provided in response to the fraudulent email requests on March 30, 2016 and included 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. This information was provided before Digilant discovered that the requests were made from a fraudulent email address. Once Digilant discovered the fraudulent nature of the attack, it immediately began an investigation to determine the nature and scope of this incident.

Notice to New Hampshire Resident

On May 4, 2016, Digilant emailed preliminary notice to all impacted individuals. This notice was provided in substantially the same form as the letter attached hereto as ***Exhibit A***. On May 5, 2016, Digilant mailed notice letters to potentially affected individuals, which includes one (1) New Hampshire

resident. The notifications provide details of the incident, information on steps individuals can take to protect against identity theft and fraud, access to one (1) year of free credit monitoring, and contact information individuals may use should they have questions or concerns. The notice letter was provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering this incident, Digilant 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. As noted above, Digilant is providing potentially affected individuals information on how to better protect against identity theft and fraud, including information on how to place a fraud alert or security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies and the IRS, and encouragement to contact the Federal Trade Commission, state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Digilant notified the FBI, and will be notifying the IRS and other appropriate state regulators. Digilant is also reviewing its policies and procedures relating to data privacy and is taking steps to further educate its staff on data privacy related issues, including email phishing and spoofing attacks.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4067.

Very truly yours,

Sian Schafle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

SMS:sn
Enclosures

EXHIBIT A

From: Rick Clemon
Sent: Wednesday, May 4, 2016 3:15 PM
To: [redacted]
Subject: Data Breach - Digilant, Inc.
Importance: High

Dear [redacted],

I am writing to inform you of an incident which may affect the security of your personal information. On May 3, 2016, we discovered that our company was the targeted victim of an email spoofing attack that compromised the security of your 2015 W-2 record, which contains your name, address, Social Security number, and 2015 compensation information. This attack occurred on March 30, 2016. We are working diligently to mitigate the impact of this event and we are notifying you so that you can take action, along with our efforts, to minimize any potential for personal financial harm. We strongly encourage you to take the preventative measures listed below to better protect against misuse of your personal information.

Through the March 30, 2016 spoofing attack, requests were made from what appeared to be a legitimate Digilant email address for 2015 employee W-2 information. Unfortunately, we remained unaware that the requests were made from a fraudulent account by an individual or individuals pretending to be an Digilant senior executive until May 3, 2016. We have been working diligently to investigate and to mitigate the impact of this attack, as well as arrange for you to have access to services and information that can be used to better protect against identity theft and fraud, if you feel it is necessary and appropriate to do so. We are also reporting this incident to the IRS and the FBI.

The confidentiality, privacy, and security of our employees' information is one of our highest priorities. While our investigation is ongoing, we feel it is important to notify you about this incident, and what we are doing to respond, as quickly as possible. We encourage you to file your tax return as soon as possible, if you have not already done so. We are reporting this incident to the IRS so that they may take steps to monitor for attempts to file fraudulent returns, or make fraudulent requests for past tax information, using Digilant employee information. If you have not yet filed your tax return, we encourage you to file an IRS Form 14039 with your 2015 return. If you have already filed and your return has been accepted by the IRS, we encourage you to consider filing the IRS Form 14039 with your 2016 return next year. 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.

In addition to offering you information on steps you can take to protect against identity theft and fraud, we will be providing all affected individuals access to one year of free credit monitoring service through Experian's® ProtectMyID Elite® product. We encourage you to follow these instructions to activate this service at no cost to you:

1. **Enroll** by: August 31, 2016 (Your code will not work after this date)
2. **Visit** the ProtectMyID website to enroll: http://www.protectmyid.com/enroll
3. **Provide** Your Activation Code: [redacted].

If you have questions or need assistance to enroll online, please call 877-441-6943 and provide engagement number: PC101296

Once you enroll, you will have access to the following features:

- **Free copy of your Experian credit report**
- **Daily 3 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
- **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded or sold.
- **Change of Address:** Alerts of any changes in your mailing address.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.
- **Identity Theft Resolution:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
- **$1 Million Identity Theft Insurance[1]:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
- **ProtectMyID ExtendCARE**: It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.

In the coming days, we will be sending a letter to your home address as reflected in our files that will offer additional resources to assist you in safeguarding against identity theft and fraud. Additionally, we will be hosting a Q&A early next week on this matter, please look for an invitation to this meeting in the coming days. We apologize for the inconvenience and concern this incident causes you. If you have any questions about the content of this notice or about this incident, please contact Rick Clemon at 844-344-4526, Ext. 705 (office) or 781-603-4575 (mobile).

Sincerely,

Rick Clemon
Chief Financial Officer

---

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG . The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

EXHIBIT B

[Digilant Letterhead]

[Date]

[First Name] [Last Name]
[Address]
[City] [State] [Zip]

Re: Notice of Data Breach

Dear [First Name] [Last Name],

I am writing as a follow-up to my May 4, 2016 email about an incident that may affect the security of some of your personal information. We take this incident very seriously and are following up to provide you with additional information on the incident and access to resources so that you can better protect against potential identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On May 3, 2016, we discovered that our company was the targeted victim of an email spoofing attack that resulted in a compromise of the security of your 2015 IRS Tax Form W-2. This attack occurred on March 30, 2016. Through this spoofing attack, requests were made from what appeared to be a legitimate Digilant email address for 2015 employee W-2 information. Unfortunately, we remained unaware that the requests were made from a fraudulent account, by an individual or individuals pretending to be a Digilant senior executive, until May 3, 2016. We have been working diligently to investigate and to mitigate the impact of the attack since we discovered the fraudulent nature of the request.

What Information Was Involved? A file that included a copy of your 2015 IRS Tax Form W-2 was sent to a fraudulent email account. An IRS Tax Form W-2 includes the following categories of information: (1) your name; (2) your address; (3) your Social Security number; and, (4) your wage information.

What We Are Doing. We take this incident, and the security of your personal information, very seriously. Digilant has security measures in place to protect the security of information in our possession. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional protections and provide additional training on safeguarding the privacy and security of information in our systems. We will also be reporting this incident to the IRS and have reported this to the FBI.

As an additional precaution, we will be providing all affected individuals access to one year of free credit monitoring service through Experian's® ProtectMyID Elite® product. Instructions on how to enroll were included in the May 4th email and are reiterated in the enclosed 'Steps You Can Take To Prevent Identity Theft And Fraud.' We encourage you to take advantage of these services by following the instructions to enroll.

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 through Experian.

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 contact Rick Clemon at 844-344-4526, Ext. 705 (office) or 781-603-4575 (mobile).

We take the privacy of the personal information in our care seriously. We sincerely regret the inconvenience and concern this incident has caused you.

Sincerely,

Rick Clemon
Chief Financial Officer

STEPS YOU CAN TAKE TO PROTECT AGAINST 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 will be providing all affected individuals access to one year of free credit monitoring service through Experian's® ProtectMyID Elite® product. We encourage you to follow these instructions to activate this service at no cost to you:

1. **Enroll** by: August 31, 2016 (Your code will not work after this date)
2. **Visit** the ProtectMyID website to enroll: http://www.protectmyid.com/enroll
3. **Provide** Your Activation Code: [activation code].

If you have questions or need assistance to enroll online, please call 877-441-6943 and provide engagement number: PC101296

Once you enroll, you will have access to the following features:

- **Free copy of your Experian credit report**
- **Daily 3 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
- **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded or sold.
- **Change of Address:** Alerts of any changes in your mailing address.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.
- **Identity Theft Resolution:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
- **$1 Million Identity Theft Insurance[1]:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
- **ProtectMyID ExtendCARE**: It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.

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

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

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 above.

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 Security Freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	888-909-8872
(NY residents call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/securityfreeze
www.equifax.com/help/credit-freeze/en_cp		

If you receive a notice from the IRS that leads you to believe that someone may have used your information, please notify the IRS's Identity Protection Specialized Unit (IPSU) immediately at 800-908-4490 or www.irs.gov/Individuals/Identity-Protection. You will also find information at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. IPSU employees are available to answer questions about identity theft and resolve any tax account issues that resulted from identity theft.

If you have not yet filed you 2015 tax return, do so as soon as possible and file an IRS Identify Theft Affidavit, IRS Form 14039, with your return. Select Box 2A on the form. By submitting this form you are formally notifying the IRS that you are a potential victim of identify fraud and would like to mark your account to identify any questionable behavior. If you have already filed your 2015 tax return and it has been accepted by the IRS, you may file the IRS Identify Theft Affidavit, IRS Form 14039, with your 2016 return next year.

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. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft/, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. 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 has not been delayed because of law enforcement.