Holland & Knight

800 17th Street, NW, Suite 1100 | Washington, DC 20006 | T 202.955.3000 | F 202.955.5564
Holland & Knight LLP | www.hklaw.com

Kaylee A. Cox
202-469-5185
kaylee.cox@hklaw.com

May 9, 2016

Attorney General Joseph Foster
NH Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

Pursuant to New Hampshire Statute, section 359-C:20, we are writing to notify you of an unauthorized acquisition of personal information involving twenty (20) New Hampshire residents.

Below is an estimated timeline of events related to Avention's investigation of this incident:

- On or around April 19, 2016, Avention began to receive reports from employees that their tax returns were being rejected due to a fraudulent return being filed in their names.
- In response, on April 19 and 20, 2016, Avention launched an investigation and contacted external third-party providers (including 401K, benefits, payroll/HR and medical providers) and also began a scan of its internal systems.
- On April 28, 2016, Avention's HRIS provider indicated that, on March 31, 2016, there was suspicious activity using legitimate user credentials (all employee I-9 Forms were accessed in one user session).
- On April 28, 2016, Avention interviewed the authorized user whose credentials were used to access the HRIS system and confirmed that the employee did not access all employee I-9 Forms.
- On April 28, 2016, Avention contacted Holland & Knight, contacted federal law enforcement, and hired a leading cybersecurity firm to assist with its investigation.
- On April 29, 2016, Avention discovered that, on April 5, 2016, an Avention employee fell victim to a phishing attack, which resulted in the unauthorized disclosure of 2015 W-

2 Forms. The Avention employee received an email, which had been manipulated to appear as if it was coming from another Avention employee; however, when replying to the email and attaching the W-2 Forms, the response was delivered to an unauthorized actor's email account.

- On April 29, 2016, Avention notified all current employees of the incident during a town hall meeting, followed by an e-mail communication.
- Avention also notified all affected former employees for whom the company had an email address via an email communication on May 4, 2016.
- The formal notification process is ongoing, and notification letters were mailed to all affected individuals on or around May 5, 2016.

The information contained on the I-9 Forms included names, addresses, Social Security Numbers, and may have included information from the identification and employment authorization documentation provided during the I-9 process, such as passport numbers, driver's license numbers, birth certificates, and/or other government-issued identification numbers. The information contained on the W-2 Forms included names, addresses, Social Security Numbers, salary information, and tax withholdings for 2015.

Avention is offering identity protection services for a period of 3 years, at no cost, to all affected individuals. Attached please find a copy of the notice letter that was mailed to the affected residents on or around May 5, 2016.

Upon learning of this incident, Avention immediately began an internal investigation, notified federal law enforcement, and took steps to notify affected individuals. Avention's investigation is currently ongoing, and, at this time, it cannot confirm that the I-9 access and the W-2 compromise are related. The company currently has no evidence to suggest that there has been any external intrusion into its computer systems. Avention is conducting a thorough review of its security measures, internal controls, and safeguards and is making changes to existing policies and procedures, including training and awareness programs, in an effort to help prevent a similar incident in the future.

Below is the contact information for Susan White, Chief Financial Officer, at Avention:

Susan White
Chief Financial Officer
Avention
300 Baker Ave.
Concord, MA 01742
978.318.4565
susan.white@avention.com

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,

Kaylee A. Cox

AVENTION
ONESOURCE SOLUTIONS
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
ACD1234
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 5, 2016

RE: Notice of Data Breach

Dear John Sample:

We are writing to let you know about two data security incidents, which are believed to have occurred on March 31, 2016 and April 5, 2016.

What Happened

On April 28, 2016, Avention learned that it suffered a data security incident, which resulted in unauthorized access to employees' I-9 Forms by an unknown source on or around March 31, 2016. Immediately upon learning this information, Avention launched an internal investigation, contacted federal law enforcement, and hired a leading cybersecurity firm to assist with our investigation. In conducting our investigation, Avention learned that, on April 5, 2016, an Avention employee fell victim to a phishing attack, which resulted in the unauthorized disclosure of 2015 W-2 Forms. The Avention employee received an email, which had been manipulated to appear as if it was coming from another Avention employee; however, when replying to the email and attaching the W-2 Forms, the response was delivered to an unauthorized actor's email account.

We have learned that several employees have had their tax returns rejected, so it appears that criminals have already attempted to misuse the information compromised. If you have already successfully filed your 2015 tax returns, the criminals would be unable to file a fraudulent return with the Internal Revenue Service ("IRS") for tax year 2015. Regardless of whether you filed already, in order to prevent and detect misuse of your information, we strongly encourage you to take the preventative measures outlined in this letter.

What Information Was Involved

The information contained on the I-9 Forms included your name, address, Social Security Number, and may have included information from the identification and employment authorization documentation you provided during the I-9 process, such as your passport number, driver's license number, birth certificate, and/or other government-issued identification number.

The information contained on your W-2 Form included your name, address, Social Security Number, salary information, and tax withholdings for 2015.

What We Are Doing

We take the protection of your information very seriously, and we sincerely apologize for what occurred here. We are taking several steps to help protect your information, including providing free identity protection services for 36 months, as described further below, and by continuing to keep you updated about this incident. As soon as the first incident was discovered, we launched an internal investigation, hired a leading cybersecurity firm to assist with our investigation, and notified federal law enforcement. A law enforcement investigation is ongoing at this time.

We are also conducting a thorough review of our security measures, internal controls, and safeguards and are making changes to existing policies and procedures, including training and awareness programs, in an effort to help prevent a similar incident in the future.

What You Can Do

We suggest that you file an IRS Form 14039, Identity Theft Affidavit (available at https://www.irs.gov/pub/irs-pdf/f14039.pdf) and **complete your 2015 tax filing process as soon as possible**. **Even** if you have **already filed** your 2015 tax return, **we still suggest you file an IRS Form 14039, Identity Theft Affidavit because it will be good for three years**. Follow the instructions in the Affidavit.

Below is language you can use on the Identity Theft Affidavit regarding why you are filing the form:

> *"My company, Avention, recently suffered a data security incident, whereby my W-2 Form was compromised. The W-2 Form contained my name, address, Social Security number, salary information, and tax withholdings for 2015."*

If the IRS or your tax preparer advises that a fraudulent tax return has been filed in your name, you will have to file a paper return, along with IRS Form 14039 (Identity Theft Affidavit) attached to the top. The return should be mailed to the address that you would use if mailing a return, which is included in the instructions for paper filings. You can obtain additional information regarding taxpayer identity theft on the IRS website, at https://www.irs.gov/Individuals/Identity-Protection and https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft, or by calling the IRS at 1-800-908-4490. For information about your state return, visit your state revenue agency's web site at http://www.taxadmin.org/state-tax-agencies.

Please note that due to these extra precautions, you may experience some delay in receiving any refund you are owed and you may be asked to take additional steps (for example, you may be provided a PIN or you may be asked to file a paper report, or even submit another copy of the Affidavit).

In addition, we recommend that you enroll in the identity protection services we are offering to you, at no charge. We are offering a **complimentary** 36-month membership of identity protection services from AllClear ID. The following identity protection services start on the date of this notice and you can use them at any time during the next 36 months. Both services are being provided to you at no charge.

> **AllClear SECURE:** This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-904-5762 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including **credit monitoring and a $1 million identity theft insurance policy**. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com using the following redemption code: Redemption Code. You may also sign up by phone by calling 1-855-904-5762.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

For More Information

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). We have also provided resources where you can obtain additional information about identity theft and ways to protect yourself. Please refer to the final page of this letter for this information.

Questions and Concerns

We sincerely apologize that this occurred, regret any inconvenience it may cause you, and encourage you to take advantage of the product outlined herein. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to call 1-855-904-5762 or contact AV-security@avention.com.

Sincerely,

Steve Pogorzelski
Chief Executive Officer

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

➢ PLACE AN EXTENDED FRAUD ALERT ON YOUR CREDIT FILE

You may also want to consider contacting the credit reporting companies and asking them to place an extended fraud alert. If you are a victim of identity theft and have created an Identity Theft Report, you can place an extended fraud alert on your credit file. It stays in effect for 7 years. When you place an extended alert, you can get 2 free credit reports within 12 months from each of the 3 nationwide credit reporting companies, and the credit reporting companies must take your name off marketing lists for prescreened credit offers for 5 years, unless you ask them to put your name back on the list.

➢ SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 877-322-8228.
Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

➢ **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➢ **BE ON THE LOOKOUT FOR PHISHING SCHEMES**

We recommend that you be on the lookout for suspicious emails. Specifically, be on the lookout for phishing schemes, which are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator.

Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (look for misspellings in the email address). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate.

➢ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft. If you believe a fraudulent tax return has been filed in your name, we recommend that you contact the Internal Revenue Service at the below information.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Internal Revenue Service, 1111 Constitution Ave NW #5480, Washington, DC 20224, 1-800-908-4490, www.irs.gov/identitytheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 36 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 36 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services (an "Event"), you must:

- notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
- fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage Under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- due to
  - any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- incurred by you from an Event that did not occur during your coverage period; or
- in connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation, fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077