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

STATE OF NH
DEPT OF JUSTICE
2016 MAR -7 AM 9:45

March 3, 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 a potential unauthorized acquisition of personal information involving two (2) New Hampshire residents.

On February 26, 2016, Information Innovators Inc. ("Triple-i") suffered a phishing attack, which resulted in the disclosure of Triple-i employees' 2015 W-2 Forms. The information contained on the W-2 Forms included employees' names, addresses, Social Security Numbers, salary information, and tax withholdings for 2015.

A Triple-i employee received an email, which had been manipulated to appear as if it was coming from another Triple-i employee. The vector of attack exploited the design of the SMTP that allows any user to forge the "FROM" address on any email and the message appeared to come from a Triple-i employee, but, when replying to the email, did not actually return to the Triple-i employee's email account. The criminal also adjusted the display name so that the Triple-i employee's name and picture was in the "TO" field in the response.

As soon as this incident was discovered, Triple-i launched an internal investigation and notified local and federal law enforcement. A law enforcement investigation is ongoing at this time. In addition, within hours of discovering this incident, Triple-i took steps to remediate the incident, including by enacting the Sender Policy Framework ("SPF"), which is a voluntary technique, aimed at reducing email spoofing. Triple-i also implemented a filter that would enforce SPF not only for the company's domain (iiinfo.com), but for all domains that provide SPF information. This technique will not only help prevent the forging and sending of Triple-i emails, but will also allow Triple-i to reject additional spam from unauthorized sources. In other words, these techniques will enable Triple-i to detect and reject forged emails from sophisticated criminals. This protocol has been implemented in combination with other anti-spam techniques that were already in place at Triple-i. Triple-i is also 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.

Currently, Triple-i has no indication of misuse of employee information as a result of this incident, but Triple-i will be notifying these individuals so that they can take steps to protect themselves. Triple-i is also offering identity protection services for a period of three years, at no cost. Attached please find a copy of the notice letter that will be mailed to the affected residents on March 3, 2016.

Below is the contact information for Andrew Adamshick, Corporate Information Security Officer (CISO) at Triple-i:

Andrew Adamshick
Information Innovators Inc.
7400 Fullerton Road, Suite 210
Springfield, VA 22153
aadamshick@iiinfo.com
571-239-6510 (cell)
571-210-7127 (office)

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

Information Innovators Inc.
Insight • Integration • Impact

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

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

March 3, 2016

RE: Notice of Data Breach

Dear John Sample:

We are writing to let you know about a data security incident, which occurred on February 26, 2016.

What Happened

Information Innovators Inc. ("Triple-i") recently suffered a phishing attack, which resulted in the unauthorized disclosure of 2015 W-2 Forms of employees and former employees who received wages in 2015.

Based on the nature of this incident, we believe the criminals may be interested in filing fraudulent tax returns. To date, we have no evidence to suggest that any employee information has been misused as a result of this incident. Further, if you have already filed your 2015 tax returns, the criminals would be unable to file a fraudulent return with the Internal Revenue Service ("IRS"). However, 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 your W-2 Form, including 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 apologize for what occurred here. We are taking several steps to help protect your information, both now and in the future, including by providing free identity protection services, as outlined herein, and by continuing to keep you updated about this incident. As soon as this incident was discovered, we launched an internal investigation and notified local and federal law enforcement. A law enforcement investigation is ongoing at this time. In addition, 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.

01-06-1-00

In addition to the steps we are taking to keep you informed and help protect your information, we are notifying you so that you can take immediate action to protect yourself. To help protect your identity, we are offering a **complimentary** three-year 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 1-877-615-3745 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 1-877-615-3745.

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

What You Can Do

If you have not yet filed your 2015 tax returns, we recommend that you file an IRS Form 14039, Identity Theft Affidavit and complete your 2015 tax filing process as soon as possible. The Identity Theft Affidavit is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. Additional information regarding taxpayer identity theft can be found on the IRS website, at https://www.irs.gov/Individuals/Identity-Protection. If you believe a fraudulent tax return has been filed in your name, we recommend that you contact the Internal Revenue Service at 1-800-908-4490.

In addition, we recommend that you enroll in the identity protection service we are offering to you, at no charge. As mentioned, you can enroll in the AllClear PRO service online at enroll.allclearid.com using the following redemption code: Redemption Code, or by phone at 1-877-615-3745.

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.

We sincerely apologize for this incident, 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 1-877-615-3745 or email idhotline@iiinfo.com.

Sincerely,

Steven Ikirt
Chief Executive Officer

Information Innovators Inc.
7400 Fullerton Road, Suite 210
Springfield, VA 22153
703.635.7088

02-06-1

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 takes 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 A 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, 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;
- 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
  - 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;
- 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; and
- 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