IceMiller
LEGAL COUNSEL

One American Square | Suite 2900 | Indianapolis, IN 46282-0200

March 21, 2016

WRITER'S DIRECT NUMBER: (317) 236-2391
INTERNET: Stephen.Reynolds@icemiller.com

Via First Class Mail

Attorney General Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

Ice Miller LLP represents YourEncore, Inc. ("YourEncore"). On March 7, 2016, as a result of a phishing email scam, 2015 W-2 tax information for current and former YourEncore employees was erroneously sent to an unauthorized third party via email. After investigating the incident, we believe that the W-2 tax form information of two (2) New Hampshire residents was transmitted to an unauthorized party. We are working with the Federal Bureau of Investigations to investigate the incident.

YourEncore sent its current and former employees a preliminary notification on March 7, 2016 and a second notification was sent on March 16, 2016 by U.S. mail and/or email. Copies of the template notification letters sent to the New Hampshire residents are attached hereto.

Please direct any questions or requests for additional information to me.

Sincerely yours,

ICE MILLER LLP

Stephen E. Reynolds, CIPP/US, CISSP
Partner

Enclosure: Copy of March 7, 2016 Notice Letter Template
Copy of March 16, 2016 Notice Letter Template

W2 Breach

Letter to W2 Employees

YourEncore takes seriously the safeguarding of your personal information. Despite our efforts, we need to disclose a recent security incident involving your information.

The morning of March 7, 2016, W-2 tax form information for calendar year 2015 for current and former YourEncore employees was erroneously sent to an unauthorized third party via email. This was in response to a phishing email scam. This breach was not a compromise of enterprise systems.

The incident was immediately discovered and the response team is actively working with the Federal Bureau of Investigation (FBI) and other private sector providers to determine responsible parties and ensure they are prosecuted to the fullest extent of the law.

For your future protection, YourEncore is contracting with a third party to provide you two years of credit monitoring and identity theft protection. Our third party vendor will send via mail information for how to enroll in these services within the next seven (7) business days and will advise you of any additional actions you may take to safeguard your personal information.

In the meantime, we want to make you aware of steps you may take immediately to guard against identity theft or fraud. Please review the enclosed Information about Identity Theft Protection.

We take the protection of your personal information seriously and are taking steps internally to prevent any future similar occurrence. We have set up a special website (http://info.yourencore.com/data-breach-response) and an internal email address, responseteam@yourencore.com to answer any additional questions you may have.

Any media, expert, internal employee or other inquiries related to this event should be forwarded to responseteam@yourencore.com. The response team includes members of the Human Resources team.

Sincerely,

Tim Tichenor
Chief Financial Officer

your encore

Important Identity Theft Protection Information

You can help safeguard yourself against identity theft or other unauthorized use of personal information by taking some simple steps.

1. **Remain vigilant**. We recommend you remain vigilant for possible incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports. Credit reports can be obtained at:

   Equifax
   1-800-685-1111
   www.equifax.com

   Experian
   1-888-397-3742
   www.experian.com

   TransUnion
   1-800-916-8800
   www.transunion.com

   If you suspect that your identity has been compromised, report suspected incidents of identity theft to local law enforcement, Federal Trade Commission, or your state attorney general. More information is available on the FTC's Web site, at www.consumer.gov/idtheft, or you can call the FTC at (877) IDTHEFT (438-4338).

2. **Look for tax-related identity theft.**

   IRS Form 14039 (https://www.irs.gov/pub/irs-pdf/f14039.pdf) permits the reporting of any event involving your personal information that may at some future time affect your federal tax records. You may wish to print the form and mail or fax it according to the instructions. In most cases, in response to such a submission, the IRS will confirm your identity and begin monitoring your federal tax account. In some cases, you may also be issued a unique Identity Protection Personal Identification Number (IP PIN) for tax filing purposes. The IP PIN is a unique six-digit number that verifies your identity at the time your

taxes are filed. You can also check with your state to see if it has a similar form to protect your state tax filings.

3. **Add fraud alerts to your credit file**. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. To place a fraud alert in your file, call one of the three nationwide credit bureaus. As soon as that bureau processes your fraud alert, it will notify the other two bureaus, which will also place fraud alerts in your file.

4. **Place a security freeze on your credit report**. You can place a security freeze on your credit report to prohibit a credit bureau from releasing information from your credit report without your prior written authorization. To do this, use the following links:

   Equifax:
   https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
   Experian: http://www.experian.com/consumer/security_freeze.html
   TransUnion: http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

your encore®

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

00002 ACD1234

00033
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 16, 2016

Dear John Sample,

On the morning of March 7, 2016, 2015 W-2 tax form information for current and former YourEncore employees was erroneously sent to an unauthorized third party via email. This was in response to a phishing email scam. This breach was not a compromise of any systems.

The incident was immediately discovered and our response team is actively working with the Federal Bureau of Investigation (FBI), outside counsel, and other third parties to determine the responsible parties.

We want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed Information about Identity Theft Prevention.

As an added precaution, we have arranged to have AllClear ID 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.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-683-1164 and a dedicated investigator will help 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 or by phone by calling 1-855-683-1164 using the following redemption code: Redemption Code.

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

We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. We have set up a special website (http://info.yourencore.com/data-breach-response) and an internal email address, responseteam@yourencore.com to answer any additional questions you may have.

Sincerely,

Tim Tichenor
Chief Financial Officer

01-03-2-00

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

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.

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

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

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

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:

- 24 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 24 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